Math 780: Elementary Number Theory
(Instructor's Notes)*

What Is It?:

- Elementary Number Theory is the study of numbers, and in particular the study of the set of positive integers.
- Does "elementary" mean "easy"? No.
- **Example.** Consider a positive integer $m < 10^5$, and view it as a four digit number (with possible leading digit 0). Suppose all four digits are distinct. Let k be the number obtained by putting the digits of m in increasing order, and let ℓ be the number obtained by putting the digits in decreasing order. Let $m' = k - \ell$. Now repeat the process with m' in place of m. Continue. What happens? How can this be explained?

Rational and Irrational Numbers:

- Define them.
- **Theorem 1.** *$\sqrt{2}$ is irrational.*
- Give typical proof.
- **Theorem 2.** *An irrational number to an irrational power can be rational.*
- **Proof:** Consider $\sqrt{2}^{\sqrt{2}}$ and $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$.
- **Theorem 3.** *e is irrational.*
- **Proof:** Assume $e = a/b$ with a and b positive integers, and set

$$(*) \qquad \theta = b!e - \sum_{j=0}^{b} \frac{b!}{j!} = \sum_{j=b+1}^{\infty} \frac{b!}{j!}.$$

Then

$$0 < \theta < \sum_{j=1}^{\infty} \frac{1}{(b+1)^j} = \frac{1}{b} \le 1.$$

On the other hand, the middle expression in $(*)$ is an integer. Hence, we have a contradiction and e is irrational.

- **Open Problem.** Is π^e irrational?
- **Open Problem.** Is $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^5}$ irrational?

*These notes are from a course taught by Michael Filaseta in the Fall of 1997.

Homework:

(1) Let $I = \mathbb{R} - \mathbb{Q}$ denote the set of irrational numbers. Determine whether each of the following is true or false. If it is true, simply state so. If it is false, state so and give a counterexample.

(a) $\alpha \in I$ and $\beta \in I$ implies $\alpha + \beta \in I$
(b) $\alpha \in I$ and $\beta \in I$ implies $\alpha\beta \in I$
(c) $\alpha \in \mathbb{Q} - \{0\}$ and $\beta \in I$ implies $\alpha + \beta \in I$ and $\alpha\beta \in I$
(d) $\alpha \in I$ and $\beta \in \mathbb{Q} - \{0\}$ implies $\alpha^\beta \in I$
(e) $\alpha \in \mathbb{Q} - \{1\}$ and $\beta \in I$ implies $\alpha^\beta \in I$

(2) Prove that $\sqrt{n}$ is irrational whenever n is a positive integer which is not a square. Give an argument similar to that given for $\sqrt{2}$. Clarify where you feel we are using certain properties of the integers that we should have perhaps discussed first.

(3) Prove that $\sqrt{2} + \sqrt{3}$ is irrational.

(4) Prove that $\sqrt{2} + \sqrt{3} + \sqrt{5}$ is irrational.

(5) Prove that $\log_2 3$ is irrational.

(6) Prove that e^2 is irrational using an argument similar to that given above for e.

Divisibility Basics:

- Definition. Let a and b be integers. Then a divides b (or a is a divisor of b or b is divisible by a) if there is an integer c such that $b = ac$.

- Notation. We write $a|b$ if a divides b, and we write $a \nmid b$ if a does not divide b.

- Definition. An integer p is prime (or is a prime) if it is > 1 and divisible by no other positive integer other than 1 and itself. (In Algebra, the condition that p be > 1 is replaced by $|p| > 1$.)

- The division algorithm.

Theorem 4. *If $a \neq 0$ and b are any integers, then there exist unique integers q (called the quotient) and r (called the remainder) with $0 \leq r < |a|$ such that $b = qa + r$.*

- **Proof.** Let r be the least non-negative integer in the double sequence

$$\dots, b - 2a, b - a, b, b + a, b + 2a, \dots.$$

Let q be such that $b - qa = r$. Since $(b - qa) - |a|$ is in the double sequence and $< b - qa$, we have $(b - qa) - |a| < 0$. Thus, $r < |a|$. Also, $r \geq 0$. This proves the existence of q and r as in the theorem.

For $j \in \{1, 2\}$, suppose q_j and r_j are integers such that $b = q_j a + r_j$ and $0 \leq r_j < |a|$. Then

$$(*) \qquad (q_1 - q_2)a - (r_1 - r_2) = 0.$$

This implies $a|(r_1 - r_2)$. On the other hand, $r_1 - r_2 \in (-|a|, |a|)$. Hence, $r_1 = r_2$. Now, $(*)$ implies $q_1 = q_2$, establishing the uniqueness of q and r as in the theorem.

• Definition and Notation. Let n and m be integers with at least one non-zero. The greatest common divisor of n and m is the greatest integer dividing both n and m. We denote it by $\gcd(n, m)$ or (n, m).

• Note that if n is a non-zero integer, then $(0, n) = |n|$.

• **Theorem 5.** *If a and b are integers with at least one non-zero, then there exist integers x_0 and y_0 such that $ax_0 + by_0 = (a, b)$. Moreover,*

$$\{ax + by : x, y \in \mathbb{Z}\} = \{k(a, b) : k \in \mathbb{Z}\}.$$

• **Proof.** Let $S = \{ax + by : x, y \in \mathbb{Z}\}$. Let d denote the smallest positive integer in S. Let x_0 and y_0 be integers for which $d = ax_0 + by_0$. Theorem 5 follows from the following claims.

Claim 1. $\{kd : k \in \mathbb{Z}\} \subseteq S$.

Reason: Clear.

Claim 2. $S \subseteq \{kd : k \in \mathbb{Z}\}$.

Reason: Let $u = ax' + by' \in S$. By Theorem 4, we have integers q and r with $u = dq + r$ and $0 \le r < d$. On the other hand,

$$r = u - dq = (ax' + by') - (ax_0 + by_0)q = a(x' - x_0 q) + b(y' - y_0 q) \in S.$$

It follows that $r = 0$ and $u = qd$.

Claim 3. $d|a$ and $d|b$.

Reason: Use Claim 2 together with $a \in S$ and $b \in S$.

Claim 4. $d = (a, b)$.

Reason: Since $ax_0 + by_0 = d$, $(a, b)|d$ so that $(a, b) \le d$. Since $d|a$ and $d|b$, d is a common divisor of a and b. By the definition of greatest common divisor, $d = (a, b)$.

The Fundamental Theorem of Arithmetic (Unique Factorization):

• **Theorem 6.** *Every integer $n > 1$ can be written uniquely as a product of primes in the form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where $p_1 < p_2 < \cdots < p_r$ are distinct primes and $e_1, e_2, \ldots, e_r$ and r are positive integers.

• **Comment:** In other words, every positive integer n can be written uniquely as a product of primes except for the order in which the prime factors occur.

• **Lemma.** *If p is a prime and a and b are integers such that $p|ab$, then either $p|a$ or $p|b$.*

• **Proof of Lemma.** Let k be an integer such that $ab = kp$, and suppose $p \nmid a$. We wish to show $p|b$. By Theorem 5, there are integers x and y such that $ax + py = 1$. Hence, $b = abx + pby = p(kx + by)$. Thus, $p|b$.

• **Proof of Theorem 6.** First, we prove that n is a product of primes by induction. The case $n = 2$ is clear. Suppose it is true for n less than some integer $m > 2$. If m is prime, then m is a product of primes. If m is not prime, then $m = ab$ with a and b integers in $(1, m)$. Since a and b are products of primes by the induction hypothesis, so is m.

Now, we prove uniqueness by induction. Again, one checks $n = 2$ directly. Suppose uniqueness of the representation of n as a product of primes as in the theorem holds for $n < m$. Let $p_1, \dots, p_r$ (not necessarily distinct) and $q_1, \dots, q_t$ (not necessarily distinct) denote primes such that $m = p_1 \cdots p_r = q_1 \cdots q_t$. Observe that $p_1 | q_1 \cdots q_t$. Hence, the lemma implies $p_1 | q_1$ or $p_1 | q_2 \cdots q_t$. This in turn implies $p_1 | q_1$, $p_2 | q_2$, or $p_1 | q_3 \cdots q_t$. Continuing, we deduce that $p_1 | q_j$ for some $j \in \{1, 2, \dots, t\}$. As p_1 and q_j are primes, we obtain $p_1 = q_j$. Now, $p_2 \cdots p_r = m/p_1 = q_1 \cdots q_{j-1} q_{j+1} \cdots q_t$ and the induction hypothesis imply that the primes $p_2, \dots, p_r$ are the same as the primes $q_1, \dots, q_{j-1}, q_{j+1}, \dots, q_t$ in some order. This implies the theorem.

Homework:

(1) Let a, b, c, and d denote positive integers. Prove each of the following:
(a) $a|b$ and $b|c$ implies $a|c$
(b) $ac|bc$ implies $a|b$
(c) $a|b$ and $c|d$ implies $ac|bd$

(2) Prove that if n is an integer ≥ 2 which is composite (i.e., not prime), then n has a prime divisor which is $\leq \sqrt{n}$.

(3) Let $S = \{\log_{10} p : p \text{ prime}\}$. Prove that the elements of S are linearly independent over the rationals. (This is an example of an infinite set of real numbers which is linearly independent over $\mathbb{Q}$.)

(4) Observe that $n^4 + 4^n$ is prime if $n = 1$. Prove that $n^4 + 4^n$ is composite if n is an integer > 1.

Euclidean Algorithm:

• Review. In grade school, we learned to compute the greatest common divisor of two numbers by factoring the numbers. For example, $(77, 119) = (7 \times 11, 7 \times 17) = 7$. Now, try $(3073531, 304313)$ this way. What's the moral?

• **Theorem 7. (The Euclidean Algorithm)** *Let a and b be positive integers. Set $r_0 = a$ and $r_1 = b$. Define $r_2, r_3, \dots, r_{n+1}$ and n by the equations*

$$\begin{array}{rcl}
r_0 = r_1 q_1 + r_2 & & \textit{with } 0 < r_2 < r_1 \\
r_1 = r_2 q_2 + r_3 & & \textit{with } 0 < r_3 < r_2 \\
\vdots & & \vdots \\
r_{n-2} = r_{n-1} q_{n-1} + r_n & & \textit{with } 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_n + r_{n+1} & & \textit{with } r_{n+1} = 0
\end{array}$$

where each q_j and r_j is in $\mathbb{Z}$. Then $(a, b) = r_n$.

- Back to examples. Compute $(3073531, 304313)$ this way. Not to be misleading, compute $(2117, 3219)$ using the Euclidean Algorithm.

- **Proof:** Let $d = (a,b)$. Then one obtains $d | r_j$ for $0 \le j \le n+1$ inductively, and hence $d | r_n$. Thus, $d \le r_n$ (since $r_n > 0$). Similarly, one obtains r_n divides r_{n-j} for $1 \le j \le n$. It follows that r_n is a divisor of a and b. By the definition of (a,b), we deduce $r_n = (a,b)$.

- Solutions to $ax + by = m$. From Theorem 5, we need only consider $m = k(a,b)$. One can find solutions when $k = 1$ by making use of the Euclidean Algorithm (backwards). Show how the complete set of solutions for general m can be obtained from this. Also, mention the connection with the simple continued fraction for a/b.

- **Example.** Solve $3219x + 2117y = 29$. The solutions are the (x, y) of the form

$$x = 25 - t \times \frac{2117}{29} \quad \text{and} \quad y = -38 + t \times \frac{3219}{29} \qquad \text{for } t \in \mathbb{Z}.$$

- **Theorem 8.** *Let a and b be positive integers. The Euclidean Algorithm for calculating (a,b) takes $\le 2([\log_2 b] + 1)$ steps (i.e, divisions).*

- **Proof:** Let $s = [\log_2 b] + 1$. In the notation of Theorem 7, we want $n \le 2s$. Assume $n \ge 2s + 1$. We show first that $r_{j+2} < r_j/2$ for $j \in \{1, 2, \dots, n-2\}$. If $r_{j+1} \le r_j/2$, then $r_{j+2} < r_{j+1} \le r_j/2$. If $r_{j+1} > r_j/2$, then $r_j = r_{j+1}q_{j+1} + r_{j+2}$ where $q_{j+1} = 1$. Hence, in this case, $r_{j+2} = r_j - r_{j+1} < r_j/2$. Hence, in either case, $r_{j+2} < r_j/2$. We deduce that

$$1 \le r_n < \frac{r_{n-2}}{2} < \frac{r_{n-4}}{4} < \cdots < \frac{r_{n-2s}}{2^s} \le \frac{r_1}{2^s} = \frac{b}{2^s}.$$

Therefore, $s < \log_2 b$. This contradicts that $s = [\log_2 b] + 1 > \log_2 b$.

Homework:

(1) For each of the following, calculate (a,b) and find a pair of integers x and y for which $ax + by = (a,b)$.

(a) $a = 289$ and $b = 1003$

(b) $a = 3569$ and $b = 1333$

(2) Find the complete set of integer solutions in x and y to

$$821x + 1997y = 24047.$$

Modulo Arithmetic:

- Definition. Two integers a and b are congruent modulo an integer n if $n | (a - b)$.

- Notation. $a \equiv b \pmod{n}$.

- **Examples.** What will be the time 1000 hours from now? On what day of the week will September 3 be in 1998?

• **Theorem 9.** *Let a, b, c, and n be integers. Then each of the following holds.*
(i) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
(ii) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.
(iii) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.
(iv) If $a \equiv b \pmod{n}$ and $d|n$, then $a \equiv b \pmod{d}$.

• **Proof:** Give the obvious proofs. In particular, in (iii), observe that $a - b = kn$ and $c - d = \ell n$ for some integers k and ℓ so that

$$ac - bd = (a-b)c + (c-d)b = (kc + \ell b)n,$$

and the result follows.

• **Comment:** Note that (iii) implies that if $a \equiv b \pmod{n}$ and k is a positive integer, then $a^k \equiv b^k \pmod{n}$.

• **Theorem 10.** *Let m be a positive integer, and let a be an integer relatively prime to m. Then there is an integer x for which $ax \equiv 1 \pmod{m}$.*

• **Proof:** Use that there are integers x and y such that $ax + my = 1$.

• **Comments:** The x in Theorem 10 is called the inverse of a modulo m. It is unique modulo m since $(a, m) = 1$ and $ax \equiv ay \mod m$ implies $x \equiv y \pmod{m}$. Also, note that if $(a, m) \neq 1$, then a does not have an inverse modulo m (since $ax - 1 = mk$ would be impossible).

• **Examples.**
(1) Explain the usual tests for divisibility by each of 2, 3, 4, 5, 6, 9, and 11.
(2) What is the last digit of 7^{1000}?
(3) Determine the last digits of the numbers in the sequence $23, 23^{23}, 23^{(23^{23})}, \dots$.
(4) Is 3752743877345287574827904870128487127731 a sum of two squares?
(5) Let $F_n = 2^{(2^n)} + 1$ (the nth Fermat number). Explain why $641|F_5$. Use that $641 = 2^4 + 5^4$ and $641 = 5 \times 2^7 + 1$.

• **Comments:** A regular n-gon is constructible with straight-edge and compass if and only if $n = 2^k p_1 \cdots p_r \geq 3$ where k and r are non-negative integers and $p_1, \dots, p_r$ are distinct Fermat primes. The only known Fermat primes are F_n for $0 \leq n \leq 4$ (i.e., 3, 5, 17, 257, and 65537), and it is believed that these are the only Fermat primes.

Homework:

(1) Prove that if $n \equiv 7 \pmod{8}$, then n is not a sum of 3 squares.

(2) Prove that for every non-constant polynomial $f(x)$ with integer coefficients, there is an integer m such that $f(m)$ is composite.

(3) A large furniture store sells 6 kinds of dining room suites, whose prices are \$231, \$273, \$429, \$600.60, \$1001, and \$1501.50, respectively. Once a South American buyer came, purchased some suites, paid the total amount due, \$13519.90, and sailed for South America. The manager lost the duplicate bill of sale and had no other memorandum of each kind of suite purchased. Help him by determining the exact number of suites of

each kind the South American buyer bought. (Don't forget to show that your solution is unique.)

(4) Find (with proof) the smallest integer > 1 dividing at least one number in the sequence $31, 331, 3331, 33331, \ldots$.

Fermat's Little Theorem:

- **Theorem 11.** *For any prime p and any integer a, $a^p - a$ is divisible by p.*

- **Comments:** In other words, with p and a as above, $a^p \equiv a \pmod{p}$. The theorem is equivalent to: if p is a prime and a is an integer with $(a,p) = 1$ (in other words, with p not dividing a), then $a^{p-1} \equiv 1 \pmod{p}$.

- **Proof 1:** Use induction. The theorem holds with $a = 1$. If it holds for a, then

$$(a+1)^p = \sum_{j=0}^{p} \binom{p}{j} a^j \equiv a^p + 1 \equiv a + 1 \pmod{p}.$$

This proves the theorem for positive integers. Since every integer is congruent to a positive integer modulo p, the result follows.

- **Proof 2:** Again, we may suppose $a > 0$. Fix a colors. The number of necklaces with p beads, each bead colored with one of the a colors (allowing repetitions), having at least two beads colored differently is $(a^p - a)/p$. Here, we count necklaces as distinct if one cannot be obtained from the other by a rotation (we don't allow flipping necklaces over). Thus, $(a^p - a)/p \in \mathbb{Z}$, and the result follows.

- Fermat's Little Theorem can be used for determining that a given integer N is composite as follows:

(i) Check N for small prime factors (this step isn't necessary but is reasonable).

(ii) Write N in base 2, say $N = \sum_{j=0}^{k} \epsilon_j 2^j$ with $\epsilon_j \in \{0,1\}$ for each j and $k = [\log N / \log 2] + 1$.

(iii) Compute $2^{2^j} \pmod{N}$ by squaring.

(iv) Calculate $m \in \{0, 1, \ldots, N-1\}$ such that

$$m \equiv \prod_{j=0}^{k} 2^{\epsilon_j 2^j} \equiv 2^N \pmod{N}.$$

(v) If $m \neq 2$, then N is composite. Otherwise the test is inconclusive.

- **Comments:** The algorithm works for establishing that "most" composite numbers are composite (i.e., for most composite numbers, $m \neq 2$). If $m = 2$, then one can check if $3^N \equiv 3 \pmod{N}$. Note that the algorithm takes on the order of $\log N$ steps so that the algorithm is a polynomial time algorithm (it runs in time that is polynomial in the length of the input - elaborate on this). There are no polynomial time algorithms that determine conclusively whether an arbitrary integer is composite.

• Definitions. A *pseudo-prime* is a composite number $n > 1$ satisfying $2^n \equiv 2 \pmod{n}$. A *probable prime* is an integer $n > 1$ satisfying $2^n \equiv 2 \pmod{n}$. (Explain the reasons behind these definitions.)

• **Examples.** Explain why $341 = 11 \times 31$ is a pseudo-prime. Explain why $F_n = 2^{2^n} + 1$ is a probable prime. (Note that for $n > 5$, F_n is really probably not a prime.)

• Definition. An *absolute pseudo-prime* (or a *Carmichael number*) is a composite number $n > 1$ such that $a^n \equiv a \pmod{n}$ for every integer a.

• **Example.** Explain why $561 = 3 \times 11 \times 17$ is an absolute pseudo-prime.

• **Comment:** Alford, Granville, and Pomerance have shown that there exist infinitely many absolute pseudo-primes. The much easier result that there exist infinitely many pseudo-primes is in the next list of homework problems.

Euler's Theorem:

• Definition and Notation. For a positive integer n, we define $\phi(n)$ to be the number of positive integers $\le n$ which are relatively prime to n. The function ϕ is called Euler's ϕ-function.

• **Examples.** $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(p) = p - 1$ for every prime p, and $\phi(pq) = (p-1)(q-1)$ for all primes p and q

• **Theorem 12.** *For every positive integer n and every integer a relatively prime to n, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.*

• **Proof:** If $n = 1$, the result is clear. We suppose as we may then that $n > 1$. Let $a_1, a_2, \dots, a_{\phi(n)}$ be the $\phi(n)$ positive integers $\le n$ relatively prime to n. Consider the numbers

$$(*) \qquad a_1 a, a_2 a, \dots, a_{\phi(n)} a.$$

Note that no two numbers in $(*)$ are congruent modulo n since $(a, n) = 1$ and $a_i a \equiv a_j a \pmod{n}$ implies $a_i \equiv a_j \pmod{n}$ so that $i = j$. Now, fix $j \in \{1, 2, \dots, \phi(n)\}$. There are integers q and r such that $a_j a = nq + r$ and $0 \le r < n$. Since $(a_j a, n) = 1$ and $n > 1$, we obtain $r \ne 0$ and $(r, n) = 1$. Thus, $r = a_k$ for some $k \in \{1, 2, \dots, \phi(n)\}$. Hence, for each $j \in \{1, 2, \dots, \phi(n)\}$, there is a $k \in \{1, 2, \dots, \phi(n)\}$ for which $a_j a \equiv a_k \pmod{n}$. Since the numbers $a_j a$ are distinct modulo n, we deduce that the numbers in $(*)$ are precisely $a_1, a_2, \dots, a_{\phi(n)}$ in some order. Therefore,

$$a_1 a_2 \cdots a_{\phi(n)} \equiv (a_1 a)(a_2 a) \cdots (a_{\phi(n)} a) \equiv a^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} \pmod{n}.$$

Since $\gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$, we obtain $a^{\phi(n)} \equiv 1 \pmod{n}$ as desired.

Wilson's Theorem:

• **Theorem 13.** *For every prime p, $(p-1)! \equiv -1 \pmod{p}$.*

• **Proof:** If $p = 2$, the result is clear. We consider now the case $p > 2$. Let $S = \{1, 2, \dots, p-1\}$. For every $a \in S$, there is a unique $a' \in S$ satisfying $a'a \equiv 1 \pmod{p}$.

If $a = 1$ or $a = p - 1$, then $a' = a$. The converse statement also holds since $a' = a$ implies $(a-1)(a+1) = a^2 - 1$ is divisible by p so that $a \equiv 1 \pmod{p}$ or $a \equiv p - 1 \pmod{p}$. The remaining elements of S can be grouped in $(p-3)/2$ pairs (a, a'), say $(a_1, a_1'), \dots, (a_{(p-3)/2}, a_{(p-3)/2}')$, so that

$$(p-1)! \equiv 1 \times (p-1) \times (a_1 a_1') \cdots (a_{(p-3)/2} a_{(p-3)/2}') \equiv 1 \times (p-1) \equiv -1 \pmod{p}.$$

• **Comment:** The converse of Wilson's Theorem also holds (see homework problem (4) below).

Homework:

(1) Prove that 1105 and 1729 are absolute pseudo-primes.

(2) Prove that if n is a pseudo-prime, then $2^n - 1$ is a pseudo-prime. (Note that this implies that there are infinitely many pseudo-primes.)

(3) Find the smallest positive integer k such that $a^k \equiv 1 \pmod{756}$ for every integer a which is relatively prime to 756.

(4) Prove the converse of Wilson's Theorem. More specifically, prove that if n is an integer > 1 for which $(n-1)! \equiv -1 \pmod{n}$, then n is a prime.

(5) Let p and d be integers with $p > 1$ and $d > 0$. Prove that p and $p + d$ are both prime if and only if

$$(p-1)! \left(\frac{1}{p} + \frac{(-1)^d d!}{p+d} \right) + \frac{1}{p} + \frac{1}{p+d}$$

is an integer.

Public-Key Encryption:

• **Example.** The following information is made public:

> If someone wishes to send me, Jim, a message, use the following. Let $N = 49601$ and $s = 247$. As your alphabet use 00 for a blank, 01 for "a", 02 for "b", 03 for "c", etc. (Eg. "No" would be represented "1415".) Suppose your message is M. Let
>
> $$E \equiv M^s \pmod{N}$$
>
> where $0 \le E < N$. Then M is your actual message, and E is the encrypted message. Publish E in the personals tomorrow, and I alone will know your actual message M.

Note: To do this properly, one needs N to be considerably larger. Here, only two letter words can actually be sent (though a combination of two letter words including blanks can make for a sentence).

• The secret. The number N is a product of two large primes (sufficiently large so only Jim knows how N factors). In the example above, $N = 193 \times 257$. Since Jim knows how N factors, he can also compute $\phi(N)$. In this case,

$$\phi(N) = \phi(193 \times 257) = 192 \times 256 = 49152.$$

Using the Euclidean algorithm, for example, Jim also knows a positive integer t such that

$$st \equiv 1 \pmod{\phi(N)}.$$

Here, $t = 199$. Thus, Jim (and only Jim) can calculate

$$E^t \equiv M^{st} \equiv M^{k\phi(N)+1} \equiv M \pmod{N}.$$

In other words, Jim can figure out M given the value of E.

- **Comment:** This approach makes for a good public-key encryption scheme because the value of $\phi(N)$ cannot *seemingly* be computed without the knowledge of how N factors. To clarify, it is possible to compute $\phi(N)$ without having the factorization of N, but the fastest known methods at the time for computing $\phi(N)$ when N is large involve first factoring N.

- Further example. Someone has sent the encrypted message $E = 48791$ to Jim. What should he do (assuming he wants to know what the message says)? Note that

$$t = 199 = 2^7 + 2^6 + 2^2 + 2 + 1.$$

By squaring, he computes

$$\begin{aligned} E &\equiv 48791 \pmod{N} \\ E^2 &\equiv 11287 \pmod{N} \\ E^{2^2} &\equiv 21001 \pmod{N} \\ E^{2^3} &\equiv 39510 \pmod{N} \\ E^{2^4} &\equiv 47029 \pmod{N} \\ E^{2^5} &\equiv 18251 \pmod{N} \\ E^{2^6} &\equiv 28286 \pmod{N} \\ E^{2^7} &\equiv 33666 \pmod{N}. \end{aligned}$$

Hence,

$$\begin{aligned} M &\equiv E^t \equiv E^{2^7} E^{2^6} E^{2^2} E^2 E^1 \\ &\equiv (33666)(28286)(21001)(11287)(48791) \equiv 809 \pmod{N}. \end{aligned}$$

The message sent was, “Hi”.

Homework:

(1) Someone wants to send Jim the message, “No”. Compute the encrypted message E and then verify your work by decoding E. (Show your work using steps similar to that shown above.)

Certified Signatures:

• The problem. Jim has two friends, Brian and Jason. Jim just got an encrypted message E in the personals. I won't specify what E was because it might upset Jim (since you can now decode Jim's messages because you too know how N factors). The message to Jim in the personals read:

> Jim, I really like your idea for having secret messages sent to you so that no one else can know what's being said in the personals besides you. In fact, I liked it so much that I thought I would send you a quick note to let you know what I think of you. Here it is: E. Sincerely, Brian.

In the above message, E is actually some number. The problem is that when Jim decoded E, he was not very happy about what Brian had to say (and you wouldn't be either if you happened to be the one the message E was intended for). As a consequence, Jim and Brian never talked to each other again, and Jim's best friend became Jason. What Jim never did figure out though was that Jason actually wrote the message.

• Solution. One can sign a message simply by adding ones name to the end of a message M and then encrypting the whole message, name and all. Unfortunately, this is precisely what Jason did; he added Brian's name to the end of the message sent to Jim. When Jim read it, he actually thought that Brian must have sent it since no one else could possibly have encrypted Brian's name. He never realized that actually anyone could encrypt Brian's name. There is however a proper way to certify a signature in an encrypted message. Let's suppose that Brian and Jason also decided to use the same encrypting scheme as Jim. In particular, Brian has some number N' that he alone knows how to factor and some number s', both of which he makes public. And suppose he has computed t' (his secret exponent for decoding messages sent to him) satisfying $s't' \equiv 1 \pmod{\phi(N')}$. Note that $S = 0218090114$ represents Brian's name. Brian computes the value of $T \equiv S^{t'} \pmod{N'}$ with $0 \le T < N'$. Since t' is only known to Brian, T is something only Brian knows. If Brian wants to truly sign a message to Jim (so that Jim knows it is from him) he now simply adds T to the end of his message and then encrypts the entire message (with T). When Jim receives the message, he decodes it. To verify the message is from Brian, he takes the value of the signature T given at the end of the message and computes $T^{s'}$ modulo N' (note that both s' and N' are known to him). Since $s't' \equiv 1 \pmod{\phi(N')}$, Jim obtains S this way (i.e., $S \equiv T^{s'} \pmod{N'}$). He then sees that the message is from Brian. The main point is that since t' is only known to Brian, he alone could have computed the value of T given at the end of the message to Jim.

• The rest of the story. Actually, Brian did have numbers N' and s' that he made public, and Jason had such numbers as well. Jason sent a friendly message to Brian which Jason signed with a certified signature. Brian responded with a message containing his own certified signature. It was then that Jason sent his message to Jim. At that point, Brian had given Jason the value of T (Brian's certified signature), so Jason used Brian's certified signature in his message to Jim. So how might this problem be avoided? (Discuss possible answers.)

The Chinese Remainder Theorem:

- **Theorem 14.** *Let $m_1, \dots, m_k$ be pairwise relatively prime positive integers. Let $b_1, \dots, b_k$ be arbitrary integers. Then the system*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $m_1 \cdots m_k$.

- **Proof (Constructive):** Let $M = m_1 \cdots m_k$. For $j \in \{1, 2, \dots, k\}$, define $M_j = M/m_j$. If i and j are in $\{1, 2, \dots, k\}$ with $i \neq j$, then $(m_i, m_j) = 1$. It follows that for each $j \in \{1, 2, \dots, k\}$, $(M_j, m_j) = 1$ so that there is an $M'_j \in \mathbb{Z}$ such that

$$M_j M'_j \equiv 1 \pmod{m_j}.$$

We set $x = \sum_{j=1}^{k} b_j M_j M'_j$. Then

$$x \equiv b_j M_j M'_j \equiv b_j \pmod{m_j} \qquad \text{for } j \in \{1, 2, \dots, k\}.$$

This proves the existence of a solution to the system of congruences in the statement of the theorem.

For uniqueness, suppose that y also satisfies $y \equiv b_j \pmod{m_j}$ for each $j \in \{1, 2, \dots, k\}$. Then $y - x \equiv 0 \pmod{m_j}$ for each such j, and we deduce that each m_j divides $y - x$. As the m_j are relatively prime, we obtain $M|(y-x)$. In other words, $y \equiv x \pmod{m_1 \cdots m_k}$.

- **Examples.**

(1) Solve $17x \equiv 3 \pmod{210}$ by using the Chinese Remainder Theorem. Use that $210 = 2 \times 3 \times 5 \times 7$ and observe that solving $17x \equiv 3 \pmod{210}$ is equivalent to solving the system $x \equiv 1 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv -1 \pmod 5$, and $x \equiv 1 \pmod 7$. The latter is equivalent to $x \equiv 1 \pmod{14}$ and $x \equiv 9 \pmod{15}$. Therefore,

$$x \equiv 1 \times 15 \times 1 + 9 \times 14 \times (-1) \equiv -111 \equiv 99 \pmod{210}.$$

(2) If a and b are integers, then the point (a, b) is called a *lattice point*. A *visible* lattice point is one for which $\gcd(a, b) = 1$ (it is visible from the origin). Prove that there are circles (or squares) in the plane which are arbitrarily large and have the property that each lattice point in the circles (or squares) is not visible. (Use that there are infinitely many primes.)

(3) Prove that there exists a positive integer k for which $2^n k + 1$ is composite for all positive integers n. (It is known that $k = 78557$ has this property and it is an open problem to determine whether or not 78557 is the smallest such k.) We use the Fermat

numbers $F_n = 2^{2^n} + 1$. Recall that F_n is prime for $0 \le n \le 4$ and F_5 is composite with 641 a "proper" divisor. Explain the following implications:

$$\begin{array}{lllll}
n \equiv 1 \pmod{2} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{3} & \text{provided} & k \equiv 1 \pmod{3}, \\
n \equiv 2 \pmod{4} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{5} & \text{provided} & k \equiv 1 \pmod{5}, \\
n \equiv 4 \pmod{8} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{17} & \text{provided} & k \equiv 1 \pmod{17}, \\
n \equiv 8 \pmod{16} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{257} & \text{provided} & k \equiv 1 \pmod{257}, \\
n \equiv 16 \pmod{32} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{65537} & \text{provided} & k \equiv 1 \pmod{65537}, \\
n \equiv 32 \pmod{64} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{641} & \text{provided} & k \equiv 1 \pmod{641}, \\
n \equiv 0 \pmod{64} & \Longrightarrow & 2^n k + 1 \equiv 0 \pmod{F_5/641} & \text{provided} & k \equiv -1 \pmod{F_5/641}.
\end{array}$$

By the Chinese Remainder Theorem, there are infinitely many positive integers k satisfying the conditions on k on the right above (note that the last modulus is relatively prime to the others). Also, every integer n can be seen to satisfy at least one of the congruences involving n on the left. It follows that there are infinitely many positive integers k such that for every positive integer n, the number $2^n k + 1$ is divisible by one of 3, 5, 17, 257, 65537, 641, and $F_5/641$. If k is sufficiently large with this property, then it will suffice for a value of k for this example

• **Comments:** If every integer n satisfies at least one of a set of congruences $x \equiv a_j \pmod{m_j}$, for $j = 1, \dots, k$, then the congruences are said to form a covering of the integers. It is unkown whether or not there is a covering consisting of distinct odd moduli > 1. Also, it is not known whether or not there is a constant $C > 0$ such that every covering using distinct moduli contains a modulus $< C$.

Homework:

(1) Find the smallest positive integer $n > 2$ such that 2 divides n, 3 divides $n+1$, 4 divides $n+2$, 5 divides $n+3$, and 6 divides $n+4$. Prove your answer is the least such n.

(2) A *squarefree number* is a positive integer n which is not divisible by a square > 1. For example, 1, 2, 3, 5, and 6 are squarefree but 4, 8, 9, and 12 are not. Let k be an arbitrary positive integer. Prove that there is a positive integer m such that $m+1, m+2, \dots, m+k$ are each NOT squarefree. (Use that there are infinitely many primes.)

(3) Calculate the remainder when the number $123456789101112\dots19781979$ is divided by 1980.

(4) Let $a_0 = a$ and $a_1 = b$ be positive integers, and let $a_{n+1} = 2a_n + a_{n-1}$ for all positive integers n. Find relatively prime a and b such that every a_n, with $n \ge 0$, is composite. (Hint: I used the system of congruences $n \equiv 0 \pmod{2}$, $n \equiv 1 \pmod{3}$, $n \equiv 3 \pmod{4}$, $n \equiv 5 \pmod{6}$, and $n \equiv 9 \pmod{12}$. You should convince yourselves that this system forms a covering of the integers. The idea is to make each a_n divisible by a prime where the prime depends on which of these congruences n satisfies. For example, suppose I choose a and b so that $a \equiv 1 \pmod{3}$ and $b \equiv -1 \pmod{3}$. Then for n satisfing $n \equiv 3 \pmod{4}$, which is one of the congruences in the system above, we will have that a_n is divisible by

3. To see this consider the sequence a_n modulo 3 keeping in mind that $a \equiv 1 \pmod 3$ and $b \equiv -1 \pmod 3$. The main problem should be figuring out what primes to use.)

Euler's Phi Function Revisited:

- Recall $\phi(n)$ is the number of positive integers $\leq n$ that are relatively prime to n.
- **Lemma 1.** *For every prime p and every positive integer k, $\phi(p^k) = p^k - p^{k-1}$.*
- **Proof.** The number of multiples of p which are $\leq p^k$ is p^{k-1}. The result follows.
- **Lemma 2.** *For relatively prime positive integers m and n, $\phi(mn) = \phi(m)\phi(n)$.*
- **Proof.** If $m = 1$ or $n = 1$, then the result is clear; so we suppose $m > 1$ and $n > 1$. Let $a_1, \dots, a_{\phi(m)}$ denote the positive integers $\leq m$ which are relatively prime to m, and let $b_1, \dots, b_{\phi(n)}$ denote the positive integers $\leq n$ which are relatively prime to n. Suppose now that $k \in \{1, 2, \dots, mn\}$ and $(k, mn) = 1$. Define a and b by

$$k \equiv a \pmod m, \quad 0 \leq a < m, \quad k \equiv b \pmod n, \quad \text{and} \quad 0 \leq b < n.$$

Since $k = a + tm$ for some integer t and since $(k, m) = 1$, we deduce that $(a, m) = 1$. Similarly, $(b, n) = 1$. Hence, there are $i \in \{1, 2, \dots, \phi(m)\}$ and $j \in \{1, 2, \dots, \phi(n)\}$ such that

$$k \equiv a_i \pmod m \qquad \text{and} \qquad k \equiv b_j \pmod n.$$

Since there are $\phi(m)\phi(n)$ choices of pairs (i, j) and k is uniquely determined by the above congruences (i.e., because of the Chinese Remainder Theorem), we get $\phi(mn) \leq \phi(m)\phi(n)$.

Now, fix a pair (i, j) with $i \in \{1, 2, \dots, \phi(m)\}$ and $j \in \{1, 2, \dots, \phi(n)\}$, and consider the integer $k \in \{1, 2, \dots, mn\}$ (that exists by the Chinese Remainder Theorem) which satisfies $k \equiv a_i \pmod m$ and $k \equiv b_j \pmod n$. There exists an integer t such that $k = a_i + tm$ so that, since $(a_i, m) = 1$, we obtain $(k, m) = 1$. Also, $(k, n) = 1$. Hence, $(k, mn) = 1$. Therefore, since each pair (i, j) corresponds to a different k, $\phi(mn) \geq \phi(m)\phi(n)$. Combining the inequalities, we get $\phi(mn) = \phi(m)\phi(n)$.

- **Theorem 15.** *Suppose $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $e_1, \dots, e_r$, and r are positive integers and $p_1, \dots, p_r$ are distinct primes. Then*

$$\phi(n) = \prod_{j=1}^{r} (p_j^{e_j} - p_j^{e_j - 1}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

- **Proof.** The second equality is clear and the first follows from Lemma 1 and Lemma 2 (using $\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r})$).
- **Examples.** Use the theorem to show that $\phi(100) = 40$ and $\phi(140) = 48$.
- A "sieve" proof of Theorem 15 can be given that doesn't make use of the lemmas. Observe that a positive integer m is not relatively prime to n if and only if m is divisible by some p_j with $j \in \{1, 2, \dots, r\}$. For distinct $j_1, \dots, j_k$ in $\{1, 2, \dots, r\}$, the number of positive multiples of $p_{j_1} \cdots p_{j_k}$ which are $\leq n$ is $n/(p_{j_1} \cdots p_{j_k})$. The inclusion-exclusion principle

implies that the number of positive integers $\le n$ which are not divisible by $p_1, \dots, p_{r-1}$, or p_r is

$$n - \sum_{j=1}^{r} \frac{n}{p_j} + \sum_{j_1<j_2\le r} \frac{n}{p_{j_1}p_{j_2}} - \sum_{j_1<j_2<j_3\le r} \frac{n}{p_{j_1}p_{j_2}p_{j_3}} + \dots + (-1)^r \frac{n}{p_1p_2\cdots p_r} = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right).$$

The theorem follows.

• **Comments:** An open problem due to Carmichael is to determine whether or not there is a positive integer n such that if m is a positive integer different from n then $\phi(m) \ne \phi(n)$. If such an n exists, it is known that if must be $> 10^{1000}$. Some result in this direction can be obtained as follows. Observe that $n \equiv 0 \pmod 2$ since otherwise $\phi(n) = \phi(2n)$. Now, $n \equiv 0 \pmod 4$ since otherwise $\phi(n) = \phi(n/2)$. Now, $n \equiv 0 \pmod 3$ since otherwise $\phi(n) = \phi(3n/2)$; and $n \equiv 0 \pmod 9$ since otherwise $\phi(n) = \phi(2n/3)$. This approach can be extended (apparently indefinitely as long as one is willing to consider branching off into different cases).

Homework:

(1) Calculate $\phi(180)$ and $\phi(1323)$.

(2) Prove that if n is a positive integer as in the comment above, then $n > 10^{30}$. (Hint: Eventually consider two cases depending on whether $13|n$ or $13 \nmid n$.)

(3) During the year 1985, a convenience store, which was open 7 days a week, sold at least one book each day, and a total of 600 books over the entire year. Must there have been a period of consecutive days when exactly 129 books were sold?

Polynomial Basics:

• Irreducible polynomials. A non-zero polynomial $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv \pm 1$ is *irreducible* (over $\mathbb{Z}$ or in $\mathbb{Z}[x]$) if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ implies either $g(x) \equiv \pm 1$ or $h(x) \equiv \pm 1$. A non-zero polynomial $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv \pm 1$ is *reducible* if $f(x)$ is not irreducible. A non-constant polynomial $f(x) \in \mathbb{Q}[x]$ is *irreducible over* $\mathbb{Q}$ (or in $\mathbb{Q}[x]$) if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Q}[x]$ implies either $g(x)$ or $h(x)$ is a constant. A non-constant polynomial $f(x) \in \mathbb{Q}[x]$ is *reducible over* $\mathbb{Q}$ if $f(x)$ is not irreducible over $\mathbb{Q}$.

• **Examples.** The polynomial x^2+1 is irreducible over $\mathbb{Z}$ and over $\mathbb{Q}$. The polynomial $2x^2+2$ is reducible over $\mathbb{Z}$ and irreducible over $\mathbb{Q}$.

• **Comment:** Suppose $f(x) \in \mathbb{Z}[x]$ and the greatest common divisor of the coefficients of $f(x)$ is 1. Then $f(x)$ is irreducible over the integers if and only if $f(x)$ is irreducible over the rationals.

• Unique factorization in $\mathbb{Z}[x]$. It exists.

• Division algorithm for polynomials. Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ with $g(x) \not\equiv 0$, there are unique polynomials $q(x)$ and $r(x)$ in $\mathbb{Q}[x]$ such that $f(x) = q(x)g(x) + r(x)$ and either $r(x) \equiv 0$ or $\deg r(x) < \deg g(x)$. In the case where $g(x)$ is monic, the polynomials $q(x)$ and $r(x)$ will be in $\mathbb{Z}[x]$.

- **Examples.** If $f(x) = x^3 + 2x + 1$ and $g(x) = x^2 + 2$, then $q(x) = x$ and $r(x) = 1$. If $f(x) = x^4 + 4$ and $g(x) = 2x^3 - 3x^2 + 2$, then $q(x) = \frac{1}{2}x + \frac{3}{4}$ and $r(x) = \frac{9}{4}x^2 - x + \frac{5}{2}$.

- The Euclidean Algorithm. Illustrate by computing $\gcd(x^9+1, x^8+x^4+1)$. Note that this example is not meant to be typical; in general the coefficients might not be integral. If we want $\gcd(f(x), g(x))$ to be monic, then division by a constant may be necessary after performing the Euclidean algorithm.

- Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, not both $\equiv 0$, there exist polynomials $u(x)$ and $v(x)$ in $\mathbb{Q}[x]$ such that

$$f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x)).$$

The Euclidean algorithm can be used to compute such $u(x)$ and $v(x)$.

- The Remainder Theorem. The remainder when a polynomial $f(x)$ is divided by $x - a$ is $f(a)$. Observe that the division algorithm for polynomials implies that there is a polynomial $q(x) \in \mathbb{Q}[x]$ and a rational number r such that $f(x) = (x - a)q(x) + r$; the remainder theorem follows by letting $x = a$. As a corollary, we note that $(x - a)|f(x)$ if and only if $f(a) = 0$.

- The Fundamental Theorem of Algebra. A non-zero polynomial $f(x) \in \mathbb{C}[x]$ of degree n has exactly n complex roots when counted to their multiplicity. In other words, if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x]$ is a non-zero polynomial with roots (counted to their multiplicity) $\alpha_1, \alpha_2, \dots, \alpha_n$, then

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

- Elementary Symmetric Functions. Expanding the above factorization of $f(x)$ in terms of its roots, we deduce that

$$f(x) = a_n\big(x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n\big)$$

where

$$\sigma_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_n,\ \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n,\ \dots,\ \sigma_n = \alpha_1\alpha_2\cdots\alpha_n$$

(in general, σ_j is the sum of the roots of $f(x)$ taken j at a time). We deduce the formula $\sigma_j = (-1)^j a_{n-j}/a_n$ for each $j \in \{1, 2, \dots, n\}$. Any rational symmetric function of the roots $\alpha_1, \alpha_2, \dots, \alpha_n$ can be written in terms of the *elementary* symmetric functions σ_j.

- **Examples.** Discuss the values of σ_j when $f(x) = x^2 - 3x + 2 = (x - 1)(x - 2)$. Also, given $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are the roots of $f(x) = x^4 + 2x^3 - 3x + 5$, compute the value of $(1/\alpha_1) + (1/\alpha_2) + (1/\alpha_3) + (1/\alpha_4)$.

- Congruences Modulo Polynomials. Is $x^{18} - 3x^{15} + x^6 - x^4 + 2x^3 - x^2 - 2$ divisible by $x^2 + x + 1$? If not, what's the remainder? Discuss the answer(s).

Homework:

(1) Calculate $\gcd(x^5 - 3x^4 + 3x^3 - 6x^2 + 2x - 3, x^4 - 3x^3 + 2x^2 - 3x + 1)$.

(2) Let α_1, α_2, and α_3 be the roots of $x^3+x+1=0$. Calculate

$$S_k = \sum_{j=1}^{3} \alpha_j^k \quad \text{for } k = 1, 2, \dots, 10.$$

(3) Determine whether x^4+1 is a factor of $x^{25}+2x^{23}+x^{17}+x^{13}+x^7+x^3+1$ using arithmetic modulo x^4+1.

(4) Consider all lines which meet the graph on $y = 2x^4+7x^3+3x-5$ in four distinct points, say $(x_i, y_i), i = 1, 2, 3, 4$. Show that $(x_1+x_2+x_3+x_4)/4$ is independent of the line and find its value.

Polynomials Modulo Integers, Part I:

- **Theorem 16.** *Let p be an odd prime. The congruence $x^2+1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

- **Proof:** First suppose $p \equiv 1 \pmod{4}$. Then $p = 4k+1$ for some positive integer k. Thus, $(p-1)/2$ is even. By Wilson's Theorem, we obtain

$$\begin{aligned} -1 \equiv (p-1)! &\equiv 1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+1}{2}\right) \times \cdots \times (p-2) \times (p-1) \\ &\equiv 1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(-\frac{p-1}{2}\right) \times \cdots \times (-2) \times (-1) \\ &\equiv (-1)^{(p-1)/2}\left(\frac{p-1}{2}\right)!\left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

Thus, in this case, $x^2+1 \equiv 0 \pmod{p}$ has the solution $x = ((p-1)/2)!$.

Now, suppose $p \equiv 3 \pmod{4}$. Then $(p-1)/2$ is odd. Assume there is an integer x such that $x^2+1 \equiv 0 \pmod{p}$. Then $x^2 \equiv -1 \pmod{p}$ implies (since $(p-1)/2$ is odd) that

$$x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv -1 \pmod{p}.$$

This contradicts Fermat's Little Theorem. Hence, the theorem follows.

- **Corollary.** *There exist infinitely many primes $\equiv 1 \pmod{4}$.*

- Before proving the corollary, we establish

Theorem 17. *There exist infinitely many primes.*

Proof 1 (Euclid's). Assume there are only finitely many primes, say $p_1, \dots, p_r$. Then the number $p_1 \cdots p_r + 1$ is not divisible by any of the primes $p_1, \dots, p_r$, contradicting the Fundamental Theorem of Arithmetic.

Proof 2. The Fermat numbers $F_n = 2^{2^n}+1$ are odd numbers > 1 satisfying

$$F_{n+1} - 2 = \prod_{j=0}^{n} F_j.$$

Hence, they are relatively prime, so there must exist infinitely many primes.

- **Proof of Corollary.** Consider the numbers $n^2 + 1$ where n is an integer. By Theorem 16, the only primes dividing any such number are 2 and primes $\equiv 1 \pmod 4$. Thus, it suffices to show there exist infinitely many primes dividing numbers of the form $n^2 + 1$. Assume otherwise. Let $p_1, \dots, p_r$ be the primes which divide numbers of the form $n^2 + 1$. Since $(p_1 \cdots p_r)^2 + 1$ is not divisible by any of the primes $p_1, \dots, p_r$, we obtain a contradiction.

Homework:

(1) Use an argument similar to Euclid's to prove there exist infinitely many primes $\equiv 3 \pmod 4$.

(2) Let $f(x)$ be a non-constant polynomial in $\mathbb{Z}[x]$. Prove there exist infinitely many primes dividing numbers of the form $f(n)$ where $n \in \mathbb{Z}$.

(3) Let q be an odd prime, and let k be a positive integer. Let $N_k = 2^{q^k} - 1 = 2^{(q^k)} - 1$.
(a) Prove that q does not divide N_k.
(b) Let p be a prime dividing N_k. Prove that $p \equiv 1 \pmod q$.
(c) Explain why $\gcd\big(N_k, 2^{q^k(q-1)} + 2^{q^k(q-2)} + 2^{q^k(q-3)} + \cdots + 2^{q^k} + 1\big) = 1$.
(d) Observe that $x^q - 1 = (x-1)(x^{q-1} + x^{q-2} + x^{q-3} + \cdots + x + 1)$. Prove that there is a prime dividing N_{k+1} which does not divide N_k.
(e) Prove there are infinitely many primes $p \equiv 1 \pmod q$.

(4) Let n be an integer ≥ 3. Prove there exist infinitely many primes p which are not congruent to 1 modulo n.

Lagrange's Theorem:

- **Theorem 18.** *Let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0$. Let p be a prime, and let $n = \deg f$. Then either the congruence*

$$(*) \qquad f(x) \equiv 0 \pmod p$$

has at most n incongruent roots modulo p or p divides each coefficient of $f(x)$.

- **Proof.** The theorem is clearly true if $n = 0$. Let m be a positive integer, and suppose the theorem holds for $n < m$. Consider $f(x) \in \mathbb{Z}[x]$ with $\deg f = m$. If $(*)$ has no solutions, then the desired conclusion follows for $f(x)$. Suppose then that $(*)$ has a solution, say a. Hence, there is an integer k such that $f(a) = kp$. This implies that $x - a$ is a factor of $f(x) - kp$ (by the Remainder Theorem). In other words, there is a $g(x) \in \mathbb{Z}[x]$ such that $f(x) = (x-a)g(x) + kp$. Clearly, $\deg g = m - 1$. Observe that $f(x) \equiv g(x)(x-a) \pmod p$. We deduce that $f(b) \equiv 0 \pmod p$ if and only if $g(b) \equiv 0 \pmod p$ or $b \equiv a \pmod p$. Since $\deg g = m - 1$, we deduce that either there are at most $m - 1$ incongruent integers b modulo p that can satisfy $g(b) \equiv 0 \pmod p$ or every coefficient of $g(x)$ is divisible by p. In either case, the theorem follows.

- **Comment:** Theorem 18 is not true if the prime p is replaced by a composite number n. For example, $x^2 - 1 \equiv 0 \pmod 8$ has 4 incongruent solutions modulo 8. Also, $3x \equiv 0 \pmod 9$ has 3 incongruent solutions modulo 9.

• **Corollary.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n, and let p be a prime. Suppose $f(x) \equiv 0 \pmod{p}$ has n incongruent solutions modulo p, say $a_1, \dots, a_n$. Then*

$$f(x) \equiv (x - a_1) \cdots (x - a_n) \pmod{p}.$$

• **Proof.** Let $g(x) = f(x) - (x - a_1) \cdots (x - a_n)$. Since $f(x)$ is monic, $\deg g \le n - 1$. Also, $g(x) \equiv 0 \pmod{p}$ has the n incongruent solutions $a_1, \dots, a_n$ modulo p. Lagrange's Theorem implies that p divides each coefficient of $g(x)$.

• Wilson's theorem can be established with the aid of Theorem 18. Let p be a prime. We want to prove $(p-1)! \equiv -1 \pmod{p}$. Let $f(x) = x^{p-1} - 1$. By Fermat's Little Theorem and the above Corollary, we deduce

$$f(x) \equiv (x-1)(x-2) \cdots (x - (p-1)) \pmod{p}.$$

Letting $x = 0$, we obtain the desired result.

Primitive Roots:

• Definition. Let a be an integer, and let n be a positive integer with $\gcd(a, n) = 1$. The *order of a modulo n* is the least positive integer d such that $a^d \equiv 1 \pmod{n}$.

• **Comment:** With a and n as above, the order of a modulo n exists since $a^{\phi(n)} \equiv 1 \pmod{n}$. Furthermore, the order of a modulo n divides $\phi(n)$. To see this, consider integers x and y for which $dx + \phi(n)y = \gcd(d, \phi(n))$, where d is the order of a modulo n. Then it follows easily that $a^{\gcd(d,\phi(n))} \equiv 1 \pmod{n}$, and the definition of d implies that $d = \gcd(d, \phi(n))$. This in turn implies $d | \phi(n)$ as claimed.

• Definition. If an integer a has order $\phi(n)$ modulo a positive integer n, then we say that a is a *primitive root* modulo n.

• **Comment:** Given a positive integer n, it is *not* necessarily the case that there exists a primitive root modulo n. There exists a primitive root modulo n if and only if n is 2, 4, p^r, or $2p^r$ where p denotes an odd prime and r denotes a positive integer. The remainder of this section deals with the case where n is a prime, and in this case we establish the existence of a primitive root.

• **Theorem 19.** *There is a primitive root modulo p for every prime p. Furthermore, there are exactly $\phi(p-1)$ incongruent primitive roots modulo p.*

• **Lemma.** *Let n denote a positive integer. Then*

$$\sum_{d|n} \phi(d) = n,$$

where the summation is over all positive divisors of n.

• **Proof of Lemma.** Write $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where the p_j are distinct primes and the e_j are positive integers. Note that

$$\sum_{d|n} \phi(d) = \prod_{j=1}^{r} \left(1 + \phi(p_j) + \cdots + \phi(p_j^{e_j})\right).$$

Since,

$$1+\phi(p_j)+\cdots+\phi(p_j^{e_j}) = 1+(p_j-1)(1+p_j+\cdots+p_j^{e_j-1}) = p_j^{e_j},$$

we deduce that

$$\sum_{d|n}\phi(d) = \prod_{j=1}^{r} p_j^{e_j} = n.$$

- Theorem 19 is an apparent consequence of the next more general theorem.

Theorem 20. *Let p be a prime, and let d be a positive divisor of $p-1$. Then the number of incongruent integers of order d modulo p is $\phi(d)$.*

- **Proof of Theorem 20.** We first show that $x^d - 1 \equiv 0 \pmod{p}$ has exactly d incongruent solutions modulo p. By Lagrange's Theorem, it suffices to show that there is at least d incongruent solutions. Assume there are $< d$ incongruent solutions. Observe that $x^{p-1}-1 = (x^d-1)g(x)$ for some $g(x) \in \mathbb{Z}[x]$ for degree $p-1-d$. A number is a root of $x^{p-1}-1 \equiv 0 \pmod{p}$ if and only if it is a root of $x^d - 1 \equiv 0 \pmod{p}$ or $g(x) \equiv 0 \pmod{p}$. By Lagrange's Theorem, $g(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ incongruent solutions modulo p. Hence, $x^{p-1}-1 \equiv 0 \pmod{p}$ has $< d+(p-1-d) = p-1$ incongruent solutions modulo p. This contradicts Fermat's Little Theorem. Hence, $x^d - 1 \equiv 0 \pmod{p}$ must have exactly d incongruent solutions modulo p.

Next, suppose a has order d' modulo p. We show that a is a root of $x^d - 1 \equiv 0 \pmod{p}$ if and only if $d'|d$. If $d'|d$, then $d = kd'$ for some integer k so that

$$a^d - 1 \equiv (a^{d'})^k - 1 \equiv 1 - 1 \equiv 0 \pmod{p}.$$

Hence, a is a root of $x^d - 1 \equiv 0 \pmod{p}$. Now suppose we know a is a root of $x^d - 1 \equiv 0 \pmod{p}$ and we want to prove $d'|d$. There are integers q and r such that $d = d'q + r$ and $0 \le r < d$. Since

$$1 \equiv a^d \equiv a^{d'q+r} \equiv (a^{d'})^q a^r \equiv a^r \pmod{p},$$

we deduce that $r = 0$ and, hence, $d'|d$ as desired.

We proceed to prove the theorem by induction. If $d = 1$, then the theorem is clear. Suppose the theorem holds for $d < D$. Then using the above information (including the Lemma), we have

$$\begin{aligned}
D &= |\{a : a^D - 1 \equiv 0 \pmod{p}, 0 \le a < p\}| \\
&= \sum_{d'|D} |\{a : a \text{ has order } d', 0 \le a < p\}| \\
&= \sum_{\substack{d'|D \\ d'<D}} \phi(d') + |\{a : a \text{ has order } D, 0 \le a < p\}| \\
&= \sum_{d'|D} \phi(d') - \phi(D) + |\{a : a \text{ has order } D, 0 \le a < p\}| \\
&= D - \phi(D) + |\{a : a \text{ has order } D, 0 \le a < p\}|.
\end{aligned}$$

The theorem follows.

- **Comment:** If g is a primitive root modulo p, then the numbers $1, g, g^2, \ldots, g^{p-2}$ are incongruent modulo p. It follows that the numbers $1, g, g^2, \ldots, g^{p-2}$ are congruent modulo p to the numbers $1, 2, \ldots, p-1$ in some order.

- **Corollary.** *For all odd primes p, there are exactly $(p-1)/2$ non-zero incongruent squares modulo p.*

- **Proof.** If $x \equiv a^2 \pmod{p}$ for some integer a with $a \not\equiv 0 \pmod{p}$, then $x^{(p-1)/2} \equiv a^{p-1} \equiv 1 \pmod{p}$. Hence, Lagrange's Theorem implies that there are $\le (p-1)/2$ non-zero incongruent squares modulo p. On the other hand, if g is a primitive root modulo p, then the numbers $1, g^2, g^4, \ldots, g^{p-3}$ form $(p-1)/2$ non-zero incongruent squares modulo p.

- **Example.** Illustrate the above by considering $p = 7$. Here, 3 is a primitive root, and the non-zero squares are 1, 2, and 4.

- **Comment:** It is not known whether 2 is a primitive root modulo p for infinitely many primes p. On the other hand, it is known that at least one of 2, 3, and 5 is a primitive root modulo p for infinitely many primes p.

Homework:

(1) (a) Using an argument similar to that given for the proof of the lemma to Theorem 20, show that if $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ and $\sigma(n) = \sum_{d|n} d$ (i.e., $\sigma(n)$ is the sum of the positive divisors of n), then

$$\sigma(n) = \prod_{j=1}^{r} \frac{p_j^{e_j+1} - 1}{p_j - 1}.$$

(b) Let $\tau(n) = \sum_{d|n} 1$ (i.e., $\tau(n)$ is the number of positive divisors of n). With n as above and using a similar argument to the above, show that

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_r + 1).$$

(2) Let n be a positive integer. Given the notation in (1)(b) above, prove

$$\left(\sum_{d|n} \tau(d) \right)^2 = \sum_{d|n} \tau^3(d).$$

(3) Let p be a prime, let g be a primitive root modulo p, and let k be an integer. Prove that g^k is a primitive root modulo p if and only if $\gcd(k, p-1) = 1$.

(4) (a) Prove that if p is a prime $\equiv 1 \pmod{3}$, then there are exactly $(p-1)/3$ non-zero incongruent cubes modulo p.

(b) Prove that if p is a prime $\not\equiv 1 \pmod{3}$, then there are exactly $p-1$ non-zero incongruent cubes modulo p. (Hint: If g^j doesn't look like a cube, maybe $g^{j+(p-1)}$ or $g^{j+2(p-1)}$ will.)

(c) Generalize parts (a) and (b) to kth powers modulo a prime. In other words, find a precise description similar to the above for the number of kth powers modulo a prime.

Euler's Criterion:

- **Theorem 21.** *Let p be an odd prime, and let a be an integer not divisible by p. If a is a square modulo p, then $a^{(p-1)/2} \equiv 1 \pmod{p}$. If a is not a square modulo p, then $a^{(p-1)/2} \equiv -1 \pmod{p}$.*

- **Proof:** In the first line of the proof of the Corollary to Theorem 20, we saw that non-zero squares modulo p are roots of $x^{p-1} - 1 \equiv 0 \pmod{p}$. This is the first half of Theorem 21. It remains to prove now that if a is not a square modulo p, then a is a root of $x^{(p-1)/2} + 1 \equiv 0 \pmod{p}$. Observe that every integer in $\{1, 2, \dots, p-1\}$ satisfies

$$(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) \equiv x^{p-1} - 1 \equiv 0 \pmod{p}$$

so that if $a \in \{1, 2, \dots, p-1\}$, then a is a root of either $x^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ or $x^{(p-1)/2} + 1 \equiv 0 \pmod{p}$ (and not both). By Lagrange's Theorem, $x^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ can have at most $(p-1)/2$ incongruent roots. By the first part of the proof, these roots are the non-zero squares modulo p. It follows that the remaining integers in $\{1, 2, \dots, p-1\}$ must satisfy $x^{(p-1)/2} + 1 \equiv 0 \pmod{p}$, completing the proof.

- **Example.** Determine if 3 is a square modulo 31. Use that $3^3 \equiv -4 \pmod{31} \implies 3^6 \equiv 16 \pmod{31} \implies 3^9 \equiv -2 \pmod{31} \implies 3^{15} \equiv -1 \pmod{31}$. By Euler's criterion, 3 is not a square modulo 31.

Quadratic Residues:

- Definition. Let p be a prime, and let a be an integer not divisible by p. If a is a square modulo p, then a is said to be a *quadratic residue modulo p*. Otherwise, we say that a is a *quadratic nonresidue modulo p*.

- Definition. Let p be a prime, and let a be an integer. The Legendre symbol $\left(\dfrac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ 0 & \text{if } a \equiv 0 \pmod{p} \\ -1 & \text{otherwise.} \end{cases}$$

- **Comment.** For p an odd prime and a an integer, Euler's criterion is equivalent to $\left(\dfrac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

- **Theorem 22.** *Let a and b be integers, and let p be a prime. Then the following hold.*

(i) If $a \equiv b \pmod{p}$, then $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$.

(ii) If $a \not\equiv 0 \pmod{p}$, then $\left(\dfrac{a^2}{p}\right) = 1$.

(iii) $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

(iv) If p is odd, then $\sum_{a=1}^{p-1} \left(\dfrac{a}{p}\right) = 0$.

• **Proof.** The definition of the Legendre symbol immediately implies (i) and (ii). Euler's criterion implies (iii) (deal with $p = 2$ separately). Finally, (iv) follows from the fact that if p is odd, then there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues in the sum (see the Corollary to Theorem 20).

• Evaluating the Legendre symbol. One can evaluate the Legendre symbol directly from the definition or with the aid of Euler's criterion. The latter done correctly is quite efficient. Another method which works somewhat better (especially by hand) is to make use of the following three theorems.

Theorem 23. *For p an odd prime,* $\left(\dfrac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$

Theorem 24. *For p an odd prime,* $\left(\dfrac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$

Theorem 25. *If p and q are odd primes, then*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\dfrac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\dfrac{q}{p}\right) & \text{if } p \equiv q \equiv -1 \pmod 4. \end{cases}$$

• **Comment.** In some sense, only Theorem 25 is needed here as it can be shown that Theorem 23 and Theorem 24 follow as a consequence of Theorem 25.

• Theorem 23 is an immediate consequence of previous material. Euler's criterion implies

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Theorem 23 is also equivalent to Theorem 16.

• **Examples.** Show that $\left(\dfrac{-17}{79}\right) = 1$ using the above results. Hence, -17 is a quadratic residue modulo 79. Also, discuss whether $x^2 - x - 1$ factors modulo 7 and modulo 11. Describe the primes p for which $x^2 - x - 1$ factors modulo p.

• A further example. Here we show that there are no integers x and y satisfying the Diophantine equation

$$(*) \qquad y^2 = x^3 + 11.$$

Assume integers x and y exist satisfying $(*)$. By considering $(*)$ modulo 4, we deduce that $x \equiv 1 \pmod 4$ (i.e., since 0 and 1 are the only squares modulo 4). Observe that $(*)$ implies

$$y^2 + 16 = x^3 + 27 = (x+3)(x^2 - 3x + 9).$$

Since $x \equiv 1 \pmod 4$, we deduce $x^2 - 3x + 9 \equiv 3 \pmod 4$. This implies that there is a prime $p \equiv 3 \pmod 4$ dividing $x^2 - 3x + 9$ and, hence, $y^2 + 16$. This implies $\left(y \times 4^{-1}\right)^2 \equiv -1 \pmod p$. This contradicts Theorem 23. Hence, $(*)$ has no integer solutions.

Homework:

(1) Calculate the Legendre symbols $\left(\dfrac{30}{71}\right)$ and $\left(\dfrac{-56}{103}\right)$.

(2) Let p denote a prime. Prove that there is a solution to $x^2 - 3x + 3 \equiv 0 \pmod p$ if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

(3) Prove that for every prime p, there is an $a \in \{1, 2, \dots, 9\}$ such that both a and $a + 1$ are squares modulo p.

(4) Prove that there are no integers x and y such that $y^2 = x^3 + 7$.

(5) (a) For every odd prime p, prove either $\left(\dfrac{-1}{p}\right) = 1$, $\left(\dfrac{2}{p}\right) = 1$, or $\left(\dfrac{-2}{p}\right) = 1$.

(b) Prove that $x^4 + 1$ is reducible modulo p for every prime p.

(6) Prove that for every positive integer N, there is an integer a such that a is not a square modulo p for every odd prime $p \le N$. (Hint: Use a major theorem from earlier in this course.)

(7) Note that 107 and $(107 - 1)/2 = 53$ are primes.

(a) Calculate the Legendre symbol $\left(\dfrac{15}{107}\right)$.

(b) The value of 15^{53} is either 1 or -1 modulo 107. Use Euler's criterion together with part (a) to determine (with explanation) whether $15^{53} \equiv 1 \pmod{107}$ or $15^{53} \equiv -1 \pmod{107}$.

(c) Using part (b), explain why 15 is a primitive root modulo 107.

Gauss' Lemma and the Proof of Theorem 24:

- **Theorem 26.** *Let p be an odd prime, and let a be an integer not divisible by p. Let n denote the number of integers in the set $S = \{a, 2a, 3a, \dots, ((p-1)/2)a\}$ which have a remainder $> p/2$ when divided by p. Then*

$$\left(\frac{a}{p}\right) = (-1)^n.$$

- **Comment:** Observe that Theorem 23 is a consequence of Theorem 26.
- Before proving Theorem 26, we explain its connection to Theorem 24.

Proof of Theorem 24 assuming Theorem 26. Here $a = 2$ and $S = \{2, 4, 6, \dots, p-1\}$. If $p \equiv 1 \pmod 4$, then the elements of S which have a remainder $> p/2$ when divided by p are $((p-1)/2) + 2k$ for $k = 1, 2, \dots, (p-1)/4$. Hence, $n = (p-1)/4$ and we obtain

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \\ -1 & \text{if } p \equiv -3 \pmod 8. \end{cases}$$

If $p \equiv 3 \pmod 4$, then the elements of S which have a remainder $> p/2$ when divided by p are $((p-1)/2) + 2k - 1$ for $k = 1, 2, \dots, (p+1)/4$. Thus, $n = (p+1)/4$ and we obtain

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = \begin{cases} 1 & \text{if } p \equiv -1 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8). \end{cases}$$

This completes the proof.

- **Proof of Theorem 26.** Let $a_1, \dots, a_n$ be the elements of S which have a remainder $> p/2$ when divided by p. Let $b_1, \dots, b_m$ be the remaining elements of S. Let a'_j (for $1 \le j \le n$) and b'_j (for $1 \le j \le m$) be defined by

$$a'_j \equiv a_j \pmod p, \quad 0 \le a'_j < p, \quad b'_j \equiv b_j \pmod p, \quad \text{and} \quad 0 \le b'_j < p.$$

Let $T = \{p - a'_j : 1 \le j \le n\} \cup \{b'_j : 1 \le j \le m\}$.

We begin by showing that $T = \{1, 2, \dots, (p-1)/2\}$. Note that $T \subseteq \{1, 2, \dots, (p-1)/2\}$ and that $n + m = (p-1)/2$. Hence, it suffices to show the $n + m$ elments defining T are distinct. If u and v are in $\{1, 2, \dots, (p-1)/2\}$ and $ua \equiv va \pmod p$, then $u \equiv v \pmod p$. It follows that the n values of $p - a'_j$ are distinct and the m values of b'_j are distinct. Assume $k \in \{1, 2, \dots, n\}$ and $\ell \in \{1, 2, \dots, m\}$ are such that $p - a'_k = b'_\ell$. Then there are u and v in $\{1, 2, \dots, (p-1)/2\}$ such that $p - ua \equiv va \pmod p$. This implies $(u+v)a \equiv 0 \pmod p$ which contradicts that $p \nmid a$ and $2 \le u + v \le p - 1$. We deduce that $T = \{1, 2, \dots, (p-1)/2\}$.

From $T = \{1, 2, \dots, (p-1)/2\}$, we obtain

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv (p - a'_1) \cdots (p - a'_n) b'_1 \cdots b'_m \equiv (-1)^n a'_1 \cdots a'_n b'_1 \cdots b'_m \\ &\equiv (-1)^n a (2a)(3a) \cdots \left(\left(\frac{p-1}{2}\right) a\right) \equiv (-1)^n a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod p.\end{aligned}$$

Therefore, by Euler's criterion,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv (-1)^n \pmod p,$$

and Theorem 26 follows.

The Quadratic Reciprocity Law:

- **Lemma.** *If p is an odd prime and a is an odd integer with p not dividing a, then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}$$

where $[\,]$ denotes the greatest integer function.

• Proof. We use the notation given in the proof of Theorem 26. For each $k \in \{1, 2, \ldots, (p-1)/2\}$, we have

$$ka = q_k p + t_k \quad \text{with} \quad 1 \leq t_k \leq p-1,$$

where if $t_k > p/2$ then t_k is some a'_j and if $t_k < p/2$ then t_k is some b'_j. Observe that $q_k = [ka/p]$. Thus,

$$(*) \qquad \sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] p + \sum_{j=1}^{n} a'_j + \sum_{j=1}^{m} b'_j.$$

Recall that

$$\{p - a'_j : 1 \leq j \leq n\} \cup \{b'_j : 1 \leq j \leq m\} = \{1, 2, \ldots, (p-1)/2\}.$$

Hence,

$$\sum_{k=1}^{(p-1)/2} k = \sum_{j=1}^{n} (p - a'_j) + \sum_{j=1}^{m} b'_j.$$

Combining this with $(*)$ gives

$$(a+1) \sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] p + pn + 2 \sum_{j=1}^{m} b'_j.$$

Since a and p are odd, we obtain $\displaystyle\sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] \equiv n \pmod 2$. The result now follows from Theorem 26.

• Proof of Theorem 25. If $p = q$, then the result is clear. So suppose $p \neq q$. It suffices to prove in this case that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\dfrac{p-1}{2} \times \dfrac{q-1}{2}}.$$

Consider the rectangle R in the xy-plane with vertices $(0,0)$, $(p/2, 0)$, $(p/2, q/2)$, and $(0, q/2)$. The number of lattice points strictly inside R is $\dfrac{p-1}{2} \times \dfrac{q-1}{2}$. We now count these points in a different way. Let D denote the diagonal joining $(0,0)$ to $(p/2, q/2)$. Thus, D is a segment of the line $py = qx$. If (x_0, y_0) is a lattice point on this line, then $p | x_0$. Therefore, (x_0, y_0) is not strictly inside R. It follows that the number of lattice points strictly inside R is the number of such points below D plus the number of such points above D. The number of such lattice points below D is $\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right]$, and the number of such lattice points above D is $\sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right]$. We deduce that

$$\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right] = \frac{p-1}{2} \times \frac{q-1}{2}.$$

The lemma now implies

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{k=1}^{(q-1)/2} \left[\frac{kp}{q}\right]} = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}},$$

completing the proof.

Homework:

(1) Let $\omega(n)$ denote the number of incongruent solutions to $x^2 \equiv 1 \pmod{2^n}$. Observe that $\omega(1) = 1$, $\omega(2) = 2$, and $\omega(3) = 4$. Prove that $\omega(n) = 4$ for all $n \geq 3$. (Indicate clearly where you use that $n \geq 3$.)

Sums of Two Squares:

- **Theorem 27.** *A positive integer n is a sum of two squares if and only if every prime $p \equiv 3 \pmod 4$ satisfies $p^e || n$ for some even number e.*

- **Proof.** First, we show that if n is a sum of two squares and $p^{2k+1} || n$ for some non-negative integer k, then either $p = 2$ or $p \equiv 1 \pmod 4$. Write $n = p^{2k+1}m$ for some integer m not divisible by p. Let a and b be such that $n = a^2 + b^2$. Let ℓ be the non-negative integer satisfying $p^\ell || a$, and write $a = p^\ell a'$ so that $a' \in \mathbb{Z}$ and $p \nmid a'$. If $\ell \geq k+1$, then

$$b^2 = n - a^2 = p^{2k+1}m - p^{2\ell}(a')^2 = p^{2k+1}(m - p^{2\ell-2k-1}(a')^2).$$

This is impossible since p does not divide $m - p^{2\ell-2k-1}(a')^2$ and $p^{2k+1} | b^2 \implies p^{2k+2} | b^2$. Thus, $\ell \leq k$ and $p^{2\ell} || (n - a^2)$. In other words, $b = p^\ell b'$ where b' is an integer not divisible by p. From $n = a^2 + b^2$ and $p^{2k+1} | n$, we deduce $(a')^2 + (b')^2 \equiv 0 \pmod p$. Hence, $(a'(b')^{-1})^2 \equiv -1 \pmod p$. By Theorem 23, we conclude as desired that either $p = 2$ or $p \equiv 1 \pmod 4$.

Now, suppose that every prime $p \equiv 3 \pmod 4$ satisfies $p^e || n$ for some even number e. Observe that $2 = 1^2 + 1^2$ (i.e., 2 is a sum of two squares). We want to show that n is a sum of two squares. It suffices to show (i) if k and ℓ are both sums of two squares, then so is $k\ell$, (ii) if $p \equiv 3 \pmod 4$, then p^2 is the sum of two squares, and (iii) if $p \equiv 1 \pmod 4$, then p is the sum of two squares. To prove (i), let a, b, a', and b' be integers such that

$k = a^2 + b^2$ and $\ell = (a')^2 + (b')^2$. Then $k = (a + b\mathrm{i})(a - b\mathrm{i})$ and $\ell = (a' + b'\mathrm{i})(a' - b'\mathrm{i})$ so that

$$\begin{aligned} k\ell &= (a + b\mathrm{i})(a' + b'\mathrm{i})(a - b\mathrm{i})(a' - b'\mathrm{i}) \\ &= ((aa' - bb') + (ab' + a'b)\mathrm{i})((aa' - bb') - (ab' + a'b)\mathrm{i}) = (aa' - bb')^2 + (ab' + a'b)^2. \end{aligned}$$

To prove (ii), simply observe that $p^2 = 0^2 + p^2$ is the sum of two squares. We now turn to establishing (iii). Since $p \equiv 1 \pmod 4$, there is an integer x_0 such that $x_0^2 \equiv -1 \pmod p$. Let $m = [\sqrt{p}]+1$ so that $\sqrt{p} < m < \sqrt{p}+1$. In particular, $m^2 > p$ which implies $m^2 \ge p+1$. Let $S_1 = \{k \in \mathbb{Z} : |k| \le m-1\}$. Since $|S_1| = 2m-1$ and $2m-1+m(m-2) = m^2-1 \ge p$, we can find $m-2$ sets $S_2, \dots, S_{m-1}$ satisfying

$$S_1 \cup S_2 \cup \cdots \cup S_{m-1} = \{-(m-1), -(m-2), \dots, -1, 0, 1, \dots, p-m-1, p-m\}$$

with each S_j consisting of $\le m$ consecutive integers and with every two S_i and S_j with $1 \le i < j \le m-1$ being disjoint. Observe that for every integer t there is a unique $j \in \{1, 2, \dots, m-1\}$ such t is congruent modulo p to some element of S_j. Consider the m numbers sx_0 where $0 \le s \le m-1$. By the pigeonhole principal, some two of these, say ux_0 and vx_0, are congruent modulo p to elements in the same S_j. Fix such u, v, and j. If $j = 1$ and $uv \ne 0$, then reassign the value of u so that $u = 0$. It follows that $(v-u)x_0$ is congruent modulo p to some element in S_1. Let $k = |v-u|$ so that $k \in \{1, 2, \dots, m-1\}$ and kx_0 is congruent modulo p to some element in S_1. Let $a \equiv kx_0 \pmod p$ with $a \in S_1$, and set $b = k$. Then

$$a^2 + b^2 \equiv k^2(x_0^2 + 1) \equiv 0 \pmod p.$$

Also,

$$|a^2 + b^2| \le (m-1)^2 + (m-1)^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p.$$

Since $b = k \ge 1$, we obtain $a^2 + b^2 \in (0, 2p)$. Since $a^2 + b^2$ is divisible by p, we deduce $a^2 + b^2 = p$. This completes the argument for (iii) and completes the proof of the theorem.

Polynomial Congruences Modulo Composite Numbers:

• Reduction to prime powers. We have dealt with solving quadratic polynomials modulo primes; we deal now with the general congruence $f(x) \equiv 0 \pmod m$ where $f(x) \in \mathbb{Z}[x]$ and $m = p_1^{e_1} \cdots p_r^{e_r}$ with the p_j denoting distinct primes and the e_j denoting positive integers. Given an integer x_0, it is easy to see that $f(x_0) \equiv 0 \pmod m$ if and only if $f(x_0) \equiv 0 \pmod{p_j^{e_j}}$ for every $j \in \{1, 2, \dots, r\}$. In other words, solving the congruence $f(x) \equiv 0 \pmod m$ is the same as solving the system of congruences $f(x) \equiv 0 \pmod{p_j^{e_j}}$ with $j \in \{1, 2, \dots, r\}$. We discuss an approach to solving $f(x) \equiv 0 \pmod{p^e}$. Once this congruence can be solved, we can piece together the solution with different prime powers by using the Chinese Remainder Theorem. The third example below illustrates how this is done.

• Solving congruences modulo prime powers. Let $f(x) \in \mathbb{Z}[x]$, and let p be a prime. To find the roots of $f(x)$ modulo a power of p, we first find the solutions to $f(x) \equiv 0 \pmod p$

and inductively increase the exponent of p in the modulus. For this purpose, suppose that e is an integer ≥ 2, we know the solutions to the congruence $f(x) \equiv 0 \pmod{p^{e-1}}$, and we want to know the solutions to $f(x) \equiv 0 \pmod{p^e}$. We begin with an integer x_0 satisfying $f(x_0) \equiv 0 \pmod{p^{e-1}}$ and determine the integers $u \equiv x_0 \pmod{p^{e-1}}$ for which $f(u) \equiv 0 \pmod{p^e}$. All integers u satisfying $f(u) \equiv 0 \pmod{p^e}$ can be obtained this way as such u also satisfy $f(u) \equiv 0 \pmod{p^{e-1}}$. Since $u \equiv x_0 \pmod{p^{e-1}}$, there is an integer k such that $u = x_0 + kp^{e-1}$. We may further suppose that $k \in \{0, 1, \dots, p-1\}$ since $f(u) \equiv 0 \pmod{p^e}$ holds if and only if $f(u + \ell p^e) \equiv 0 \pmod{p^e}$ holds for every integer ℓ. From Calculus, we can write

$$f(x + kp^{e-1}) = f(x) + f'(x)kp^{e-1} + \frac{f''(x)}{2!}(kp^{e-1})^2 + \cdots .$$

Observe that there are a finite number of terms on the right-hand side above and that $f^{(\ell)}(x)/\ell! \in \mathbb{Z}[x]$ for every positive integer ℓ. Note that $e \geq 2$ implies $2(e-1) \geq e$. Hence,

$$(*) \qquad 0 \equiv f(x_0 + kp^{e-1}) \equiv f(x_0) + f'(x_0)kp^{e-1} \pmod{p^e}.$$

If $f'(x_0) \equiv 0 \pmod{p}$ and $f(x_0) \equiv 0 \pmod{p^e}$, then $(*)$ is true for all integers k. If $f'(x_0) \equiv 0 \pmod{p}$ and $f(x_0) \not\equiv 0 \pmod{p^e}$, then $(*)$ is not true regardless of k. If $f'(x_0) \not\equiv 0 \pmod{p}$, then $f'(x_0)$ has an inverse modulo p. Also, $f(x_0) \equiv 0 \pmod{p^{e-1}}$ so $p^{e-1} | f(x_0)$. In this case, $(*)$ has the unique solution $k \in \{0, 1, \dots, p-1\}$ given by

$$(**) \qquad k \equiv -\frac{f(x_0)}{p^{e-1}} f'(x_0)^{-1} \pmod{p}.$$

Summarizing, we have that for a given solution x_0 of $f(x) \equiv 0 \pmod{p^{e-1}}$, one of the following occurs:

(i) $f'(x_0) \equiv 0 \pmod{p}$ and $f(x_0) \equiv 0 \pmod{p^e}$ and there are p incongruent solutions u modulo p^e to $f(x) \equiv 0 \pmod{p^e}$ with $u \equiv x_0 \pmod{p^{e-1}}$ and they are given by $u = x_0 + kp^{e-1}$ where $k \in \{0, 1, \dots, p-1\}$,

(ii) $f'(x_0) \equiv 0 \pmod{p}$ and $f(x_0) \not\equiv 0 \pmod{p^e}$ and there do not exist solutions u to $f(x) \equiv 0 \pmod{p^e}$ with $u \equiv x_0 \pmod{p^{e-1}}$, or

(iii) $f'(x_0) \not\equiv 0 \pmod{p}$ and there is exactly one solution u modulo p^e to $f(x) \equiv 0 \pmod{p^e}$ with $u \equiv x_0 \pmod{p^{e-1}}$ and it is given by $u = x_0 + kp^{e-1}$ with k satisfying $(**)$.

• Two examples. Let $f(x) = x^2 + x + 1$ and $p = 3$. Then $f(1) \equiv 0 \pmod{3}$. In fact, every integer satisfying $f(x) \equiv 0 \pmod{3}$ is congruent to 1 modulo 3. Since $f'(x) = 2x+1$, we deduce that $f'(1) \equiv 0 \pmod{3}$ and $f(1) \equiv 3 \not\equiv 0 \pmod{3^2}$. By (ii), $f(x) \equiv 0 \pmod{3^2}$ has no solutions and so neither does $f(x) \equiv 0 \pmod{3^e}$ for each $e \geq 2$.

Now, suppose $f(x) = x^2 + 4x + 4$ and $p = 3$. Note that modulo 3, $f(x)$ is the same here as in the previous problem. Again, all solutions to $f(x) \equiv 0 \pmod{3}$ are 1 modulo 3. Also, $f'(1) \equiv 0 \pmod{3}$ and $f(1) \equiv 0 \pmod{3^2}$. Thus, by (i), there are three incongruent solutions to $f(x) \equiv 0 \pmod{3^2}$ given by 1, 4, and 7. Observe that if x_0 represents any one of these three solutions, then $f'(x_0) \equiv f'(1) \equiv 0 \pmod{3}$. Also, $f(1) \equiv 9 \not\equiv 0 \pmod{3^3}$,

$f(4) \equiv 36 \not\equiv 0 \pmod{3^3}$, and $f(7) \equiv 81 \equiv 0 \pmod{3^3}$. By (i) and (ii), there exist exactly three incongruent solutions to $f(x) \equiv 0 \pmod{3^3}$ given by 7, 16, and 25. Observe that solving $f(x) \equiv 0 \pmod{3^e}$ is actually easy since $f(x) = (x+2)^2$. If k is the least integer greater than or equal to $e/2$, then $f(x) \equiv 0 \pmod{3^e}$ if and only if $x + 2 \equiv 0 \pmod{3^k}$. It follows that $f(x) \equiv 0 \pmod{3^e}$ has exactly 3^{e-k} solutions given by $3^k\ell - 2$ where $\ell \in \{1, 2, \dots, 3^{e-k}\}$.

- A third example. Here we calculate all incongruent solutions modulo 175 to

$$x^3 + 2x^2 + 2x - 6 \equiv 0 \pmod{175}.$$

Since $175 = 5^2 \times 7$, we consider $f(x) \equiv 0 \pmod{25}$ and $f(x) \equiv 0 \pmod{7}$ where $f(x) = x^3 + 2x^2 + 2x - 6$. Since $f(x) \equiv (x-3)(x^2+2) \pmod{5}$ and $\left(\dfrac{-2}{5}\right) = -1$, the only solutions of $f(x) \equiv 0 \pmod{5}$ are 3 modulo 5. Since $f'(3) \equiv 41 \equiv 1 \not\equiv 0 \pmod{5}$ and $f(3) = 45$, we obtain from (iii) that the all solutions to $f(x) \equiv 0 \pmod{25}$ are congruent to $3 + 5(-9) \equiv 8$ modulo 25. One checks directly that the incongruent solutions modulo 7 to $f(x) \equiv 0 \pmod{7}$ are 2, 4, and 6. It follows that there are exactly three incongruent solutions modulo 175, say x_1, x_2, and x_3, satisfying

$$\begin{array}{lll} x_1 \equiv 8 \pmod{25}, & x_2 \equiv 8 \pmod{25}, & x_3 \equiv 8 \pmod{25} \\ x_1 \equiv 2 \pmod{7}, & x_2 \equiv 4 \pmod{7}, & x_3 \equiv 6 \pmod{7}. \end{array}$$

By the proof of the Chinese Remainder Theorem,

$$\begin{aligned} x_1 &\equiv 8 \times 7 \times (-7) + 2 \times 25 \times 2 \equiv -392 + 100 \equiv -292 \equiv 58 \pmod{175}, \\ x_2 &\equiv 8 \times 7 \times (-7) + 4 \times 25 \times 2 \equiv x_1 + 100 \equiv 158 \pmod{175}, \text{ and} \\ x_3 &\equiv 8 \times 7 \times (-7) + 6 \times 25 \times 2 \equiv x_2 + 100 \equiv 83 \pmod{175}. \end{aligned}$$

Thus, $f(x) \equiv 0 \pmod{175}$ has exactly three incongruent solutions modulo 175 given by 58, 83, and 158.

Homework:

(1) Find all the incongruent solutions modulo 135 to $x^5 + x^3 + 5x + 15 \equiv 0 \pmod{135}$. Do this in the method described above showing your work as in the third example.

Tossing Coins Over The Phone:

- Two people A and B agree over the phone to get together at either A's house or B's house, but each is too lazy to volunteer going over to the other's house. Since B is thinking rather quickly, he says, "I'll toss a coin and you call heads or tails. If you are right, I'll come over to your house. If you are wrong, you have to come over here." It so happens that A is thinking even better, and she suggests the following fair way to toss a coin over the phone.

Step 1: A forms a number $n = pq$ where p and q are distinct large primes congruent to 3 modulo 4. The primes are small enough that they can pass current primality tests and large enough so that n cannot be factored using current factoring methods. A tells B what the value of n is.

Step 2: B chooses $k \in \{1, 2, \dots, n-1\}$, computes $\ell \equiv k^2 \pmod{n}$ with $\ell \in \{1, 2, \dots, n-1\}$, and tells A what ℓ is. (We suppose that $\gcd(k, pq) = 1$; since p and q are large, this is very likely. In any case, the coin toss is not perfect because of this assumption.)

Step 3: A tries to figure out what k is. She knows $\ell \equiv k^2 \pmod{p}$ and $\ell \equiv k^2 \pmod{q}$. Note that $p \equiv 3 \pmod{4}$ so that $(p+1)/4 \in \mathbb{Z}$. The value of $\pm k$ modulo p can be determined by computing $k_1 \equiv \ell^{(p+1)/4} \pmod{p}$. To see this, observe that

$$k_1^2 \equiv \left(\ell^{(p+1)/4}\right)^2 \equiv \ell^{(p+1)/2} \equiv \ell^{(p-1)/2}\ell \equiv k^{p-1}\ell \equiv \ell \pmod{p}.$$

Note that Lagrange's Theorem implies the incongruent solutions of $x^2 \equiv \ell \pmod{p}$ are precisely $\pm k$ modulo p. Hence, $k_1 \equiv \pm k \pmod{p}$. Also, A computes $k_2 \equiv \ell^{(q+1)/4} \pmod{q}$ so that $k_2 \equiv \pm k \pmod{q}$. Observe that the solutions modulo n of $x^2 \equiv \ell \pmod{n}$ are given by

$$\begin{array}{rlcl}
\text{(i)} & x \equiv k_1 \pmod{p} & \text{and} & x \equiv k_2 \pmod{q} \\
\text{(ii)} & x \equiv -k_1 \pmod{p} & \text{and} & x \equiv -k_2 \pmod{q} \\
\text{(iii)} & x \equiv k_1 \pmod{p} & \text{and} & x \equiv -k_2 \pmod{q} \\
\text{(iv)} & x \equiv -k_1 \pmod{p} & \text{and} & x \equiv k_2 \pmod{q}
\end{array}$$

A computes $u \in \{1, 2, \dots, n-1\}$ satisfying (i) and $v \in \{1, 2, \dots, n-1\}$ satisfying (iii). Then the solution to (ii) is $x \equiv -u \pmod{n}$ and the solution to (v) is $x \equiv -v \pmod{n}$. Note that $v \not\equiv \pm u \pmod{n}$ as $u + v$ is not divisible by p and $u - v$ is not divisible by q. Since $k^2 \equiv \ell \pmod{n}$, we deduce that either $k \equiv \pm u \pmod{n}$ or $k \equiv \pm v \pmod{n}$ but not both. A selects one of u or v, say w, and tells B that she is guessing that k is one of w and $n - w$.

Step 4: B checks if k is one of w and $n - w$. If it is, then B admits it (so he has to go over to her place). If k is not one of w and $n - w$, then B tells A that she was incorrect. In this event the conversation continues as B must convince A that he is not lying. To prove that B is telling the truth, B tells A how n factors. B determines this as follows. Suppose $w = u$ (in the case that $w = v$, the factorization of n is determined in a similar way) so that $k \equiv \pm v \pmod{n}$. From the definition of u and v, it follows that $w + k$ is divisible by exactly one of p and q. Hence, B can determine p or q by computing $\gcd(n, w + k)$. (Observe that B does not know which of the two numbers u and $n - u$ given to him is w, but either one can be used since $\gcd(n, n - w + k)$ is also either p or q.) This easily enables B to factor n. Thus, in the event that B claims that A's guess of w or $n - w$ for k is incorrect, B verifies that A is incorrect by giving A the factorization of n.

Definitions and Notations for Analytic Estimates:

• Let f and g be real-valued functions with domain containing an interval $[c, \infty)$ for some real number c. We say that *$f(x)$ is big oh of $g(x)$* and write $f(x) = O(g(x))$ if there is a constant $C > 0$ such that $|f(x)| \le Cg(x)$ for all x sufficiently large. We say *$f(x)$ is less than less than $g(x)$* and write $f(x) \ll g(x)$ if $f(x) = O(g(x))$, and we say *$f(x)$ is greater than greater than $g(x)$* and write $f(x) \gg g(x)$ if $g(x) = O(f(x))$. We say *the asymptotic order of $f(x)$ is $g(x)$* and write $f(x) \asymp g(x)$ (or $f(x) \gg\ll g(x)$) if $g(x) \ll f(x) \ll g(x)$. We say that *$f(x)$ is little oh of $g(x)$* and write $f(x) = o(g(x))$ if $\displaystyle\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. We say that *$f(x)$ is aymptotic to $g(x)$* and write $f(x) \sim g(x)$ if $\displaystyle\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. Analogous definitions exist if the domain is in the set of positive integers.

• **Examples.** Discuss each of the following:

$$\sum_{k=1}^{n} k \asymp n^2, \qquad \sum_{k=1}^{n} k \sim \frac{n^2}{2}, \qquad \sqrt{x+1} - \sqrt{x} \ll \frac{1}{\sqrt{x}}, \qquad \log\left(1 + \frac{1}{x}\right) = O(1/x).$$

• **Comment:** The expression $O(g(x))$ in an equation represents a function $f(x) = O(g(x))$. To clarify, the last equation in

$$\sum_{p\le x} \left[\frac{x}{p}\right] = \sum_{p\le x} \frac{x}{p} + O\biggl(\sum_{p\le x} 1\biggr) = \sum_{p\le x} \frac{x}{p} + O(x)$$

does not assert that a function is $O\biggl(\displaystyle\sum_{p\le x} 1\biggr)$ if and only if it is $O(x)$ but rather there is a function $f(x)$ that satisfies $f(x) = O\biggl(\displaystyle\sum_{p\le x} 1\biggr)$ and $f(x) = O(x)$. Indeed, in the equation above, the big oh expressions both represent the same function $f(x) = \displaystyle\sum_{p\le x} \left(\left[\frac{x}{p}\right] - \frac{x}{p}\right)$.

• An estimate using integrals. Explain why $\displaystyle\sum_{k\le x} \frac{1}{k} \ge \log x$.

Homework:

(1) Let $f : \mathbb{R}^+ \to \mathbb{R}^+$ and $g : \mathbb{R}^+ \to \mathbb{R}^+$. Find all possible implications between the following. In each case, give a proof or a counterexample.

(a) $f(x) \sim g(x)$
(b) $f(x) = g(x) + O(1)$
(c) $f(x) - g(x) \asymp 1$
(d) $f(x) = g(x) + o(g(x))$

(2) (a) Prove that $\displaystyle\sum_{k\le x} \frac{1}{k} \le 1 + \log x$ for all $x \ge 1$.

(b) Prove that $\sum_{k\le x} \frac{1}{k} \sim \log x$.

(c) Prove that $\sum_{k\le x} \frac{1}{k} = \log x + O(1)$.

(3) (a) How many positive integers ≤ 210 are not divisible by each of the primes 2, 3, 5, and 7? For example, 11 would be such an integer but 39 would not be.

(b) Let $A(x) = |\{n \le x : \text{each of } 2, 3, 5, \text{ and } 7 \text{ does not divide } n\}|$. Prove that $A(x) \sim cx$ for some constant c and determine the value of c.

(4) Let a be a real number. Suppose $f : [a, \infty) \to \mathbb{R}$ has the property that for every $t \ge a$, there exists an $M(t)$ such that $|f(x)| \le M(t)$ for all $x \in [a, t]$. Suppose $g : [a, \infty) \to \mathbb{R}^+$ has the property that for every $t \ge a$, there exists an $\varepsilon(t) > 0$ such that $g(x) \ge \varepsilon(t)$ for all $x \in [a, t]$. Finally, suppose that $f(x) \ll g(x)$. Prove that there is a constant $C > 0$ such that $|f(x)| \le Cg(x)$ for all $x \ge a$.

(5) Let $f : \mathbb{R}^+ \to \mathbb{R}$ and $g : \mathbb{R}^+ \to \mathbb{R}^+$ be Riemann integrable functions. Suppose that $f(t) = O(g(t))$. Prove or disprove that

$$\int_1^x f(t)\,dt = O\bigg(\int_1^x g(t)\,dt\bigg).$$

Sums and Products Involving Primes:

- **Lemma.** $\prod_{p\le x}\left(1 - \frac{1}{p}\right) \le \frac{1}{\log x}$ *for all* $x > 1$.
- **Proof.** The lemma follows from

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} = \prod_{p\le x}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) \ge \sum_{k\le x}\frac{1}{k} \ge \log x.$$

- **Comment:** Observe that the lemma gives another proof that there are infinitely many primes.

- **Theorem 28.** *The series* $\sum_{p \text{ prime}} \frac{1}{p}$ *diverges. In fact,* $\sum_{p\le x}\frac{1}{p} \gg \log\log x$.
- **Proof.** For $x > 1$, the lemma implies

$$-\log\prod_{p\le x}\left(1-\frac{1}{p}\right) \ge \log\log x.$$

On the other hand,

$$\begin{aligned}\log\prod_{p\le x}\left(1-\frac{1}{p}\right) &= \sum_{p\le x}\log\left(1-\frac{1}{p}\right) = -\sum_{p\le x}\left(\frac{1}{p}+\frac{1}{2p^2}+\frac{1}{3p^3}+\cdots\right)\\ &\ge -\sum_{p\le x}\left(\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right) = -\sum_{p\le x}\frac{1}{p}+C(x),\end{aligned}$$

where

$$|C(x)| = \left| -\sum_{p\le x} \frac{1}{p(p-1)} \right| \le \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1.$$

Hence,

$$\sum_{p\le x} \frac{1}{p} \ge -\log \prod_{p\le x} \left(1 - \frac{1}{p}\right) - 1 \ge \log\log x - 1 \gg \log\log x.$$

- **Comment:** The sum of the reciprocals of every prime ever written down is < 4.
- **Theorem 29.** $\displaystyle\sum_{p\le x} \frac{\log p}{p} \ll \log x.$
- **Proof.** Observe that $\displaystyle\sum_{n\le x} \log n \le x\log x$ since the sum consists of $[x]$ terms each $\le \log x$. Therefore,

$$\begin{aligned} x\log x \ge \sum_{n\le x} \log n \ge \sum_{n\le x}\sum_{p|n} \log p = \sum_{p\le x}\sum_{\substack{n\le x \\ p|n}} \log p = \sum_{p\le x} \left[\frac{x}{p}\right] \log p \\ = x\Bigg(\sum_{p\le x} \frac{\log p}{p}\Bigg) + O\Bigg(\sum_{p\le x} \log p\Bigg) = x\Bigg(\sum_{p\le x} \frac{\log p}{p}\Bigg) + O\Big(x\log x\Big). \end{aligned}$$

The result follows.

- **Theorem 30.** $\displaystyle\prod_{p\le x} \left(1 - \frac{1}{p}\right) \gg\ll \frac{1}{\log x}.$
- **Proof.** The lemma implies the $\ll$ part of the asymptotic relation. We begin in a manner similar to the proof of the lemma. We use that

$$\prod_{p\le x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p\le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \le \sum_{k\le y} \frac{1}{k} + S,$$

where y is an arbitrary number > 1 and where

$$\begin{aligned} S = \sum_{\substack{k>y \\ q|k \implies q\le x}} \frac{1}{k} \le \sum_{\substack{k>y \\ q|k \implies q\le x}} \frac{\log k}{k\log y} \\ = \frac{1}{\log y} \sum_{\substack{k>y \\ q|k \implies q\le x}} \frac{1}{k} \sum_{p^e|k} \log p = \frac{1}{\log y} \sum_{p\le x} \log p \sum_{e\ge 1} \sum_{\substack{k>y, p^e|k \\ q|k \implies q\le x}} \frac{1}{k} \\ \le \frac{1}{\log y} \sum_{p\le x}\sum_{e\ge 1} \frac{\log p}{p^e} \sum_{\substack{k\ge 1 \\ q|k \implies q\le x}} \frac{1}{k} = \frac{1}{\log y} \sum_{p\le x}\sum_{e\ge 1} \frac{\log p}{p^e} \prod_{q\le x} \left(1 - \frac{1}{q}\right)^{-1}. \end{aligned}$$

By Theorem 29, there is a constant $c > 0$ such that

$$\sum_{p \le x} \sum_{e \ge 1} \frac{\log p}{p^e} = \sum_{p \le x} \frac{\log p}{p-1} \le 2 \sum_{p \le x} \frac{\log p}{p} \le c \log x.$$

Setting $P = \prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1}$ and using the previous homework problem (2)(a), we deduce that

$$P \le 1 + \log y + \frac{c(\log x)P}{\log y} \qquad \Longrightarrow \qquad \left(1 - \frac{c \log x}{\log y}\right) P \le 1 + \log y.$$

Taking $y = x^{4c}$, we obtain $(3/4)P \le 1 + 4c \log x$ from which $P \ll \log x$ follows. This implies the $\gg$ part of the asymptotic relation in the statement of the theorem.

- **Theorem 31.** $\sum_{p \le x} \frac{1}{p} = \log \log x + O(1)$.
- **Proof.** From the proof of Theorem 28,

$$\log \prod_{p \le x} \left(1 - \frac{1}{p}\right) = -\sum_{p \le x} \frac{1}{p} + C(x) \qquad \text{where } |C(x)| \le 1.$$

By Theorem 30, there exist constants $c_1 > 0$ and $c_2 > 0$ (and we may in fact take $c_2 = 1$) such that

$$\frac{c_1}{\log x} < \prod_{p \le x} \left(1 - \frac{1}{p}\right) < \frac{c_2}{\log x}$$

provided x is sufficiently large (but note that problem (3) in the previous homework implies $x \ge 2$ will do). Hence, for x sufficiently large, it follows that

$$\log \prod_{p \le x} \left(1 - \frac{1}{p}\right) = -\log \log x + O(1).$$

We deduce then that

$$\sum_{p \le x} \frac{1}{p} = -\log \prod_{p \le x} \left(1 - \frac{1}{p}\right) + C(x) = \log \log x + O(1).$$

Homework:

(1) (a) Prove that $(\log x)^k = o(x^\varepsilon)$ for every $\varepsilon > 0$ and every $k > 0$.

(b) Part (a) implies that $\log x$ to any power grows slower than x^ε for every $\varepsilon > 0$. Find a function which grows slower than x^ε for every $\varepsilon > 0$ and also grows faster than $\log x$ to any power. In other words, find an explicit function $f(x)$ such that $f(x) = o(x^\varepsilon)$ for every

$\varepsilon > 0$ and $(\log x)^k = o(f(x))$ for every $k > 0$. Justify your answer. (Hint: Try $f(x) = e^{u(x)}$ for some appropriate $u(x)$.)

(c) Prove that $(\log\log x)^k = o((\log x)^\varepsilon)$ for every $\varepsilon > 0$ and every $k > 0$.

(d) Find with proof a function $f : \mathbb{R}^+ \to \mathbb{R}^+$ such that $x \log x = o(f(x))$ and $\sum_{n=1}^{\infty} \dfrac{1}{f(n)}$ diverges.

(2) Let p_n denote the nth prime. It is known that $p_n \sim cn\log n$ for some constant c. Using this information and Theorem 31, prove that $c = 1$.

The Number of Prime Divisors of n:

- Notation. The number of distinct prime divisors of n is denoted by $\omega(n)$.
- Definition. Let $f : \mathbb{Z}^+ \to \mathbb{R}^+$ and $g : \mathbb{Z}^+ \to \mathbb{R}^+$. Then $f(n)$ is said to have normal order $g(n)$ if for every $\varepsilon > 0$, the number of positive integers $n \le x$ satisfying

$$(1-\varepsilon)g(n) < f(n) < (1+\varepsilon)g(n)$$

is asymptotic to x (i.e., for almost all positive integers n, $f(n) \in ((1-\varepsilon)g(n), (1+\varepsilon)g(n))$).

- **Theorem 32.** *$\omega(n)$ has normal order* $\log\log n$.
- **Lemma.** $\displaystyle\sum_{n\le x} \big(\omega(n) - \log\log x\big)^2 \ll x\log\log x$.
- **Proof.** We examine each term on the right-hand side of the equation

$$\sum_{n\le x} \big(\omega(n) - \log\log x\big)^2 = \sum_{n\le x} \omega(n)^2 - 2\bigg(\sum_{n\le x} \omega(n)\bigg)\log\log x + \sum_{n\le x} (\log\log x)^2.$$

For the third term, we easily obtain

$$\sum_{n\le x} (\log\log x)^2 = x(\log\log x)^2 + O((\log\log x)^2).$$

For the second term, we use that

$$\begin{aligned}\sum_{n\le x} \omega(n) &= \sum_{n\le x}\sum_{p|n} 1 = \sum_{p\le x} \sum_{\substack{n\le x\\ n\equiv 0 \pmod p}} 1 = \sum_{p\le x} \left[\frac{x}{p}\right] \\ &= \sum_{p\le x} \frac{x}{p} + O(x) = x(\log\log x + O(1)) + O(x) = x\log\log x + O(x).\end{aligned}$$

For the first term, we take advantage of the estimate we just made to obtain

$$\begin{aligned}\sum_{n\le x} \omega(n)^2 &= \sum_{n\le x} \bigg(\sum_{p|n} 1\bigg)^2 = \sum_{n\le x}\sum_{p|n}\sum_{q|n} 1 \\ &= \sum_{n\le x}\sum_{\substack{p\ne q\\ pq|n}} 1 + \sum_{n\le x}\sum_{p|n} 1 = \sum_{n\le x}\sum_{\substack{p\ne q\\ pq|n}} 1 + x\log\log x + O(x).\end{aligned}$$

We proceed by observing that

$$\sum_{n\le x}\sum_{\substack{p\ne q\\ pq|n}} 1 = \sum_{\substack{p\ne q\\ pq\le x}}\sum_{\substack{n\le x\\ pq|n}} 1 = \sum_{\substack{p\ne q\\ pq\le x}} \left[\frac{x}{pq}\right] = \sum_{\substack{p\ne q\\ pq\le x}} \frac{x}{pq} + O(x) = \sum_{pq\le x}\frac{x}{pq} - \sum_{p\le\sqrt{x}}\frac{x}{p^2}+O(x).$$

Theorem 31 imlies that each of the sums $\sum_{p\le\sqrt{x}}(1/p)$ and $\sum_{p\le x}(1/p)$ is $\log\log x + O(1)$ so that

$$(\log\log x)^2+O(\log\log x) = \Big(\sum_{p\le\sqrt{x}}\frac{1}{p}\Big)^2 \le \sum_{pq\le x}\frac{1}{pq} \le \Big(\sum_{p\le x}\frac{1}{p}\Big)^2 = (\log\log x)^2+O(\log\log x).$$

Also, $\sum_{p\le\sqrt{x}}(1/p^2) = O(1)$ since $\sum_{p}(1/p^2)$ converges (by comparison with $\sum_{n=1}^{\infty}(1/n^2)$). We deduce that

$$\sum_{n\le x}\omega(n)^2 = x(\log\log x)^2 + O(x\log\log x).$$

Combining the above information, we obtain

$$\sum_{n\le x}\big(\omega(n)-\log\log x\big)^2 = O(x(\log\log x)).$$

• **Proof of Theorem 32.** Assume $\omega(n)$ does not have normal order $\log\log n$. Then there exist $\varepsilon > 0$ and $\delta > 0$ such that there are arbitrarily large values of x for which the number of positive integers $n \le x$ satisfying

$$(*) \qquad |\omega(n) - \log\log n| \ge \varepsilon \log\log n$$

is $> \delta x$. If $x^{1/e} < n \le x$, then

$$\log\log x \ge \log\log n > \log\log(x^{1/e}) = \log\log x - 1.$$

If, in addition, n satisfies $(*)$, then

$$|\omega(n)-\log\log x| > |\omega(n)-\log\log n| - 1 \ge \varepsilon\log\log n - 1 > \varepsilon\log\log x - (1+\varepsilon).$$

We consider x satisfying $(*)$ for $> \delta x$ positive integers $n \le x$ with x sufficiently large so that

$$\frac{\varepsilon}{2}\log\log x > 1+\varepsilon \qquad \text{and} \qquad x^{1/e} < \frac{\delta}{2}x.$$

In particular,

$$\varepsilon\log\log x - (1+\varepsilon) > \frac{\varepsilon}{2}\log\log x.$$

We deduce that there are $> \delta x - x^{1/e} > (\delta/2)x$ positive integers $n \in (x^{1/e}, x]$ for which

$$|\omega(n) - \log\log x| > \frac{\varepsilon}{2} \log\log x.$$

Hence,

$$\sum_{n \le x} \big(\omega(n) - \log\log x\big)^2 \ge \frac{\delta}{2} x \left(\frac{\varepsilon}{2} \log\log x \right)^2 \ge \frac{\delta\varepsilon^2}{8} x (\log\log x)^2.$$

Observe that we can find x arbitrarily large satisfying this inequality. We obtain a contradiction to the lemma since it implies that there is a constant $C > 0$ for which

$$\sum_{n \le x} \big(\omega(n) - \log\log x\big)^2 \le Cx \log\log x$$

for all x sufficiently large.

Homework:

(1) Prove that for every $\varepsilon > 0$, there is a constant $C(\varepsilon) > 0$ such that the number of positive integers $n \le x$ for which

$$(1 - \varepsilon) \log\log n < \omega(n) < (1 + \varepsilon) \log\log n$$

does not hold is $\le C(\varepsilon)x / \log\log x$ for all x sufficiently large.

(2) Let $f : \mathbb{Z}^+ \to \mathbb{R}^+$, and suppose that $f(n)$ has normal order $\log\log n$. Prove or disprove that the average value of $f(n)$ for $n \le x$ is asymptotic to $\log\log x$. More specifically, prove or disprove that

$$\frac{1}{x} \sum_{n \le x} f(n) \sim \log\log x.$$

(Comment: In the proof of the lemma in this section, we showed a result that is even stronger than this in the case that $f(n) = \omega(n)$.)

Chebyshev's Theorem:

- Background. Let $\pi(x)$ denote the number of primes $\le x$. Chebyshev's Theorem asserts that for all x sufficiently large

$$0.92 \left(\frac{x}{\log x} \right) < \pi(x) < 1.11 \left(\frac{x}{\log x} \right).$$

He used his result to give the first proof of Bertrand's Hypothesis that for every $x \ge 1$ there is a prime in the interval $(x, 2x]$. More specifically, the above implies that there is an x_0 such that if $x \ge x_0$, then

$$\pi(2x) - \pi(x) > 0.92 \left(\frac{2x}{\log(2x)} \right) - 1.11 \left(\frac{x}{\log x} \right) > 0.$$

Combining such an estimate with knowledge of a specific x_0 and computations verifying Bertrand's Hypothesis for $x < x_0$, a proof of Bertrand's Hypothesis follows. Similar work by others has been obtained. In particular, Ramanujan gave an argument for Bertrand's Hypothesis and noted that there are at least 5 primes in $(x, 2x]$ for $x \geq 20.5$. Our next theorem is a variation of Chebyshev's Theorem. The proof below is due to Erdős.

- **Theorem 33.** *If n is a sufficiently large positive integer, then*

$$\frac{1}{6}\left(\frac{n}{\log n}\right) < \pi(n) < 3\left(\frac{n}{\log n}\right).$$

- **Proof.** Let m be a positive integer. We begin with the inequalities

$$2^m \leq \binom{2m}{m} < 4^m.$$

The first of these inequalities follows from noting that one can choose m objects from a collection of $2m$ objects by first randomly deciding whether each of the first m objects is to be included in the choice or not. The second inequality follows from

$$4^m = (1+1)^{2m} = \sum_{j=0}^{2m} \binom{2m}{j} > \binom{2m}{m}.$$

From the above inequalities, we deduce that

$$(*) \qquad m \log 2 \leq \log((2m)!) - 2\log(m!) < m \log 4.$$

We use that if p is a prime and $p^r || k!$, then $r = [k/p] + [k/p^2] + \cdots$. Therefore,

$$(**) \qquad \log((2m)!) - 2\log(m!) = \sum_p \sum_{j=1}^{\infty} \left(\left[\frac{2m}{p^j}\right] - 2\left[\frac{m}{p^j}\right]\right) \log p.$$

It is easy to verify that $[2x] - 2[x] \in \{0, 1\}$ for every real number x. Hence, $(*)$ and $(**)$ imply

$$m \log 2 \leq \sum_{p \leq 2m} \left(\sum_{1 \leq j \leq \log(2m)/\log p} 1 \right) \log p \leq \sum_{p \leq 2m} \log(2m) = \pi(2m)\log(2m).$$

Thus, if $n = 2m$, then

$$\pi(n) \geq \frac{\log 2}{2}\left(\frac{n}{\log n}\right) > \frac{1}{4}\left(\frac{n}{\log n}\right).$$

Also, if $n = 2m + 1$, then

$$\pi(n) \geq \pi(2m) > \frac{1}{4}\left(\frac{2m}{\log(2m)}\right) \geq \frac{1}{4}\left(\frac{2m}{2m+1}\right)\frac{2m+1}{\log(2m+1)} \geq \frac{1}{6}\left(\frac{n}{\log n}\right).$$

This establishes the lower bound in the theorem (for all positive integers n).

For the upper bound, we use that if $m < p \le 2m$, then $[2m/p] - 2[m/p] = 1$. Thus, $(*)$ and $(**)$ imply

$$\begin{aligned} m \log 4 &\ge \sum_{m<p\le 2m} \left(\left[\frac{2m}{p} \right] - 2\left[\frac{m}{p} \right] \right) \log p \\ &\ge \sum_{m<p\le 2m} \log p \ge \sum_{m<p\le 2m} \log m = \big(\pi(2m) - \pi(m)\big) \log m. \end{aligned}$$

Hence,

$$\pi(2m) - \pi(m) \le (\log 4) \frac{m}{\log m}.$$

We consider positive integers r and s satisfying $2^r \le n < 2^{r+1}$ and $2^s \le n^{19/20} < 2^{s+1}$. Observe that s tends to infinity with n. Taking $m = 2^j$ above, we deduce

$$\pi(2^{j+1}) - \pi(2^j) \le (\log 4) \frac{2^j}{\log(2^j)} \le (\log 4) \frac{2^j}{\log(2^s)} \qquad \text{for } j \in \{s, s+1, \dots, r\}.$$

Summing over j, we obtain

$$\begin{aligned} \pi(n) - \pi\big(n^{19/20}\big) &\le \pi\big(2^{r+1}\big) - \pi\big(2^s\big) \le \frac{\log 4}{\log(2^s)} \Big(2^s + 2^{s+1} + \dots + 2^r \Big) \\ &\le \frac{(\log 4) 2^{r+1}}{\log(2^s)} \le \frac{2(\log 4) n}{s \log 2} = 2(\log 4) n \left(\frac{s+1}{s} \right) \frac{1}{(s+1)\log 2} \\ &\le 2(\log 4) n \left(\frac{s+1}{s} \right) \frac{1}{\log\big(n^{19/20}\big)} = \frac{40 \log 4}{19} \left(\frac{s+1}{s} \right) \frac{n}{\log n} < 2.92 \left(\frac{s+1}{s} \right) \frac{n}{\log n}. \end{aligned}$$

For n and, hence, s sufficiently large, we deduce

$$\pi(n) < 2.95 \frac{n}{\log n} + \pi\big(n^{19/20}\big) \le 2.95 \frac{n}{\log n} + n^{19/20} = \left(2.95 + \frac{\log n}{n^{1/20}} \right) \frac{n}{\log n} < 3 \left(\frac{n}{\log n} \right),$$

completing the proof.

The Prime Number Theorem and Its Generalizations:

- The Prime Number Theorem asserts that $\pi(x) \sim x/\log x$. Observe that this is stronger than Chebyshev's theorem. In this section, we mention some theorems without proving them. The first two are variations of the Prime Number Theorem.

- **Theorem 34.** $\pi(x) = \dfrac{x}{\log x} + O\left(\dfrac{x}{\log^2 x} \right)$.

- Definition and Notation. We define the logarithmic integral of x by $\mathrm{Li}(x) = \displaystyle\int_2^x \frac{dt}{\log t}$.

This varies slightly (by a constant) from historic definitions of the logarithmic integral, but the results below will not be affected by this change.

- **Theorem 35.** *For every $k > 0$, we have $\pi(x) = Li(x) + O\left(\dfrac{x}{\log^k x}\right)$ where the implied constant depends on k.*

- Theorem 35 implies Theorem 34 and more. Using integration by parts and the estimate

$$(*) \qquad \int_2^x \frac{dt}{\log^4 t} \ll \frac{x}{\log^4 x},$$

explain why Theorem 35 implies

$$\pi(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} + \frac{2x}{\log^3 x} + O\left(\frac{x}{\log^4 x}\right).$$

- Dirichlet's Theorem asserts that if a and b are positive relatively prime integers, then there are infinitely many primes of the form $a + bn$. Set

$$\pi(x; b, a) = |\{p \le x : p \equiv a \pmod{b}\}|.$$

Then a strong variation of Dirichlet's Theorem is the following.

Theorem 36. *If a and b are positive relatively prime integers and $k > 0$, then*

$$\pi(x; b, a) = \frac{1}{\phi(b)} Li(x) + O\left(\frac{x}{\log^k x}\right)$$

where the implied constant depends only on k and b.

Homework:

(1) Prove $(*)$.

(2) There is a constant A such that $\left|\pi(x) - \dfrac{x}{(\log x) + A}\right| \ll \dfrac{x}{\log^3 x}$. Determine with proof the value of A.

(3) (a) Let α and β be positive real numbers. Prove that $\displaystyle\sum_{\alpha < n \le \beta} \frac{1}{n} = \log(\beta/\alpha) + O(1/\alpha)$.

(b) Let $S = \{m_1, m_2, \dots\}$ where $m_1, m_2, \dots$ are integers satisfying $0 < m_1 < m_2 < \cdots$. Define $S(x) = |\{m \le x : m \in S\}|$ (so $S(x)$ is the number of elements in S which are $\le x$). Suppose that $\displaystyle\sum_{j=1}^{\infty} \frac{1}{m_j}$ converges. Prove that almost all integers are not in S. In other words, show that

$$\lim_{x \to \infty} \frac{S(x)}{x} = 0.$$

(c) Use Theorem 33 to show that $\displaystyle\sum_{x < p \le 20x} \frac{1}{p} \ll \frac{1}{\log x}$. (Alternatively, one can use Theorem 31, but Theorem 33 is simpler.)

(d) Let $T = \{p_1, p_2, \dots\}$ where $p_1, p_2, \dots$ are primes satisfying $p_1 < p_2 < \cdots$. Define $T(x) = |\{p \le x : p \in T\}|$. Suppose that $\sum_{j=1}^{\infty} \frac{1}{p_j}$ converges. Is it necessarily true that

$$\lim_{x \to \infty} \frac{T(x)}{\pi(x)} = 0$$

(i.e., that almost all primes are not in T)?

Riemann-Stieltjes Integrals:

• Definitions and Notations. Suppose $f : [a, b] \mapsto \mathbb{R}$. Let $\mathcal{P} = \{x_0, x_1, \dots, x_n\}$ denote a partition of $[a, b]$ with $a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b$. Let $M(\mathcal{P}) = \max_{1 \le k \le n} \{x_k - x_{k-1}\}$. Let $t_k \in [x_{k-1}, x_k]$ for $k \in \{1, 2, \dots, n\}$. Consider

$$S(\mathcal{P}, f, \{t_k\}) = \sum_{k=1}^{n} f(t_k)(x_k - x_{k-1}).$$

If $S(\mathcal{P}, f, \{t_k\})$ tends to a limit A (independent of the t_k) as $M(\mathcal{P})$ tends to zero, then we write

$$\int_a^b f(x)\, dx = A$$

and say that the Riemann integral of $f(x)$ on $[a, b]$ exists and equals A. Let $g : [a, b] \mapsto \mathbb{R}$. With the notations above, we set

$$S(\mathcal{P}, f, g, \{t_k\}) = \sum_{k=1}^{n} f(t_k)\big(g(x_k) - g(x_{k-1})\big).$$

If $S(\mathcal{P}, f, g, \{t_k\})$ tends to a limit A (independent of the t_k) as $M(\mathcal{P})$ tends to zero, then we write

$$\int_a^b f(x)\, dg(x) = A$$

and say that the Riemann-Stieltjes integral of $f(x)$ with respect to $g(x)$ on $[a, b]$ exists and equals A.

• **Comments:** The properties of Riemann integrals and Riemann-Stieltjes integrals are very similar. Note in fact that if $g(x) = x$, then the definitions coincide. If $g(x)$ is differentiable on $[a, b]$, then one can show

$$\int_a^b f(x)\, dg(x) = \int_a^b f(x) g'(x)\, dx.$$

We will mainly be interested in the case when $g(x)$ is a step function.

- **Example:** $\displaystyle\int_1^x \frac{1}{t}\,d[t] = \sum_{n=2}^{[x]} \frac{1}{n}$.

- We will make use of an integration by parts formula for Riemann-Stieltjes integrals. For a proof of this and other properties of Riemann-Stieltjes integrals (defined somewhat differently), see the instructor's notes at:

```
http://www.math.sc.edu/~filaseta/courses/Math555/Math555.html
```

Lemma: *If* $\displaystyle\int_a^b g(x)\,df(x)$ *exists, then so does* $\displaystyle\int_a^b f(x)\,dg(x)$ *and*

$$\int_a^b f(x)\,dg(x) = f(x)g(x)\Big|_a^b - \int_a^b g(x)\,df(x) = f(b)g(b) - f(a)g(a) - \int_a^b g(x)\,df(x).$$

- **Example:** We apply integration by parts to the integral in the previous example. We obtain

$$\begin{aligned}\int_1^x \frac{1}{t}\,d[t] &= \frac{[x]}{x} - \frac{[1]}{1} - \int_1^x [t]\,d(1/t) = \int_1^x \frac{[t]}{t^2}\,dt + O(1/x) \\ &= \int_1^x \frac{1}{t}\,dt - \int_1^x \frac{t-[t]}{t^2}\,dt + O(1/x) = \log x - \int_1^x \frac{\{t\}}{t^2}\,dt + O(1/x).\end{aligned}$$

Observe that $\displaystyle\int_1^x \frac{\{t\}}{t^2}\,dt \le \int_1^x \frac{1}{t^2}\,dt = 1 - \frac{1}{x}$. It follows that $\displaystyle\int_1^\infty \frac{\{t\}}{t^2}\,dt$ exists. Also,

$$\int_x^\infty \frac{\{t\}}{t^2}\,dt \le \int_x^\infty \frac{1}{t^2}\,dt = \frac{1}{x}.$$

Combining the above, we deduce

$$\int_1^x \frac{1}{t}\,d[t] = \log x - \int_1^\infty \frac{1}{t^2}\,dt + \int_x^\infty \frac{1}{t^2}\,dt + O(1/x) = \log x - \int_1^\infty \frac{1}{t^2}\,dt + O(1/x).$$

From the previous example, we obtain

$$\sum_{n\le x} \frac{1}{n} = \log x + \gamma + O(1/x) \qquad \text{where} \qquad \gamma = 1 - \int_1^\infty \frac{1}{t^2}\,dt = 0.5772157\dots.$$

More precisely, the analysis above gives

$$\sum_{n\le x} \frac{1}{n} = \log x + \gamma + E(x) \qquad \text{where} \qquad E(x) = -\frac{\{x\}}{x} + \int_x^\infty \frac{\{t\}}{t^2}\,dt.$$

Recall that this last integral is $\le 1/x$ so that we can deduce $|E(x)| \le 1/x$. Thus, for example, $\displaystyle\sum_{n\le 10^6} 1/n$ can be computed to within 10^{-6} by considering $\log\left(10^6\right)+\gamma = 14.392726\dots$.

• **Comment:** The constant γ is called Euler's constant. It is unknown whether or not γ is irrational.

Sums and Products of Primes Revisited:

• We combine the lemma from the previous section with the Prime Number Theorem to arrive at improvements to some earlier results.

Theorem 37: *There exist constants C_1, C_2, and C_3 such that*

(i) $\displaystyle\sum_{p \le x} \frac{1}{p} = \log\log x + C_1 + O\biggl(\frac{1}{\log x}\biggr)$,

(ii) $\displaystyle\sum_{p \le x} \frac{\log p}{p} = \log x + C_2 + O\biggl(\frac{1}{\log x}\biggr)$, *and*

(iii) $\displaystyle\prod_{p \le x} \biggl(1 - \frac{1}{p}\biggr) \sim \frac{C_3}{\log x}$.

• **Proof of parts (i) and (iii):** For (i), we use integration by parts and Chebyshev's Theorem to obtain

$$\sum_{p \le x} \frac{1}{p} = \int_1^x \frac{1}{t}\, d\pi(t) = \frac{\pi(x)}{x} + \int_1^x \frac{\pi(t)}{t^2}\, dt = O\biggl(\frac{1}{\log x}\biggr) + \int_2^x \frac{1}{t\log t}\, dt + C_1(x)$$

where

$$C_1(x) = \int_2^x \frac{1}{t^2}\biggl(\pi(t) - \frac{t}{\log t}\biggr)\, dt.$$

By a previous homework problem and Theorem 34,

$$\int_2^x \frac{1}{t^2}\biggl|\pi(t) - \frac{t}{\log t}\biggr|\, dt \ll \int_2^x \frac{1}{t\log^2 t}\, dt \ll 1.$$

It follows that

$$\int_2^\infty \frac{1}{t^2}\biggl(\pi(t) - \frac{t}{\log t}\biggr)\, dt = \lim_{x\to\infty} C_1(x)$$

exists. Also, observe that

$$\int_x^\infty \frac{1}{t^2}\biggl|\pi(t) - \frac{t}{\log t}\biggr|\, dt \ll \int_x^\infty \frac{1}{t\log^2 t}\, dt \ll \frac{1}{\log x}.$$

Hence,

$$\begin{aligned} C_1(x) &= \int_2^\infty \frac{1}{t^2}\biggl(\pi(t) - \frac{t}{\log t}\biggr)\, dt - \int_x^\infty \frac{1}{t^2}\biggl(\pi(t) - \frac{t}{\log t}\biggr)\, dt \\ &= \int_2^\infty \frac{1}{t^2}\biggl(\pi(t) - \frac{t}{\log t}\biggr)\, dt + O\biggl(\frac{1}{\log x}\biggr). \end{aligned}$$

Since

$$\int_2^x \frac{1}{t\log t}\,dt = \log\log x - \log\log 2,$$

we obtain (i) with

$$C_1 = \int_2^\infty \frac{1}{t^2}\left(\pi(t) - \frac{t}{\log t}\right) dt - \log\log 2.$$

For (iii), we argue along the lines of the proofs of Theorem 28 and 31. Note that

$$\log \prod_{p\le x}\left(1-\frac{1}{p}\right) = \sum_{p\le x}\log\left(1-\frac{1}{p}\right) = -\sum_{p\le x}\sum_{k=1}^{\infty}\frac{1}{kp^k} = -\sum_{p\le x}\frac{1}{p} - C_3(x),$$

where

$$C_3(x) = \sum_{p\le x}\sum_{k=2}^{\infty}\frac{1}{kp^k} \le \sum_{p\le x}\sum_{k=2}^{\infty}\frac{1}{p^k} = \sum_{p\le x}\frac{1}{p(p-1)} \le \sum_{2\le n\le x}\frac{1}{n(n-1)} \le 1.$$

We deduce that $\lim\limits_{x\to\infty} C_3(x)$ exists. Also,

$$\sum_{p>x}\sum_{k=2}^{\infty}\frac{1}{kp^k} \le \sum_{n>x}\frac{1}{n(n-1)} = \frac{1}{[x]-1} \ll \frac{1}{x}.$$

It follows that

$$C_3(x) = \sum_{p}\sum_{k=2}^{\infty}\frac{1}{kp^k} - \sum_{p>x}\sum_{k=2}^{\infty}\frac{1}{kp^k} = \sum_{p}\sum_{k=2}^{\infty}\frac{1}{kp^k} + O\left(\frac{1}{x}\right).$$

We deduce from (i) that

$$\log\prod_{p\le x}\left(1-\frac{1}{p}\right) = -\log\log x - C_1 - \sum_{p}\sum_{k=2}^{\infty}\frac{1}{kp^k} + O\left(\frac{1}{\log x}\right) = -\log\log x - C + O\left(\frac{1}{\log x}\right)$$

where $C = C_1 + \sum\limits_{p}\sum\limits_{k=2}^{\infty}\frac{1}{kp^k}$. We obtain

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) = \frac{e^{-C+O(1/\log x)}}{\log x} \sim \frac{C_3}{\log x}$$

where $C_3 = e^{-C}$.

• **Comments:** The proof of (ii) is omitted (but note the related problem in the next homework). The constants in Theorem 37 are

$$C_1 = 0.261497212847643\ldots, \qquad C_2 = -1.33258\ldots, \qquad \text{and} \qquad C_3 = 0.561459\ldots.$$

Also, the number C in the argument above can be shown to be Euler's constant. Ignoring the big-oh term in (i), it is not hard to see that if one could print a million primes per second, then it would take over 1000 years to print enough primes (assumed distinct) to make the sum of their reciprocals exceed 4. A more rigorous estimate is possible (where the error term is not ignored).

Homework:

For the problems below, you are to make use of Theorems 34, 35, and 36 as well as Riemann-Stieltjes integrals.

(1) Prove that $\displaystyle\sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$.

(2) Prove that $\displaystyle\sum_{p \le x} \log p = x + O\left(\frac{x}{\log x}\right)$.

(3) Let a and b be positive integers with $\gcd(a,b) = 1$. Prove that

$$\sum_{\substack{p \le x \\ p \equiv a \pmod{b}}} \frac{1}{p} \sim \frac{1}{\phi(b)} \log\log x.$$

(4) Let p_n denote the n^{th} prime. Prove that $p_n \sim n \log n$.

(5) Prove that there are infinitely many primes which begin and end with the digit 9. More specifically, show that there are infinitely many primes which can be written in the form $\displaystyle\sum_{k=0}^{r} d_k 10^k$ where $d_r = d_0 = 9$ and $d_k \in \{0, 1, 2, \dots, 9\}$ for each k.

Integers With Large Prime Factors:

- Definitions. Let $P(x)$ denote the number of positive integers $\le x$ having a property P. Then we say that a positive proportion of the positive integers satisfies P if there is a constant $C > 0$ such that $P(x) > Cx$ for all sufficiently large x. If there is a constant $C \ge 0$ for which $P(x) \sim Cx$, then we say the proportion of positive integers satisfying P is C. If this proportion is 1, then we say that almost all positive integers satisfy P.

- **Examples.** Almost all positive integers are composite. It follows as a consequence of our next result that the proportion of positive integers n having a prime factor $> \sqrt{n}$ is $\log 2$.

- **Theorem 38.** *The number of positive integers $n \le x$ having a prime factor $> \sqrt{n}$ is* $(\log 2)x + O\left(\dfrac{x}{\log x}\right)$.

- **Proof.** The desired quantity is

$$\sum_{n\le x}\sum_{\substack{\sqrt{n}<p\le n\\ p|n}} 1 = \sum_{p\le x}\sum_{\substack{n\le x, n<p^2\\ p|n}} 1 = \sum_{p\le\sqrt{x}}\sum_{\substack{n<p^2\\ p|n}} 1 - \sum_{\sqrt{x}<p\le x}\sum_{\substack{n\le x\\ p|n}} 1$$

$$= \sum_{p\le\sqrt{x}} (p-1) - \sum_{\sqrt{x}<p\le x}\left[\frac{x}{p}\right] = O\big(\sqrt{x}\,\pi(\sqrt{x})\big) + \sum_{\sqrt{x}<p\le x}\frac{x}{p} + O(\pi(x)).$$

Chebyshev's Theorem implies that the error terms (the big-oh terms) are both $O(x/\log x)$. Theorem 37 (i) implies

$$\sum_{\sqrt{x}<p\le x}\frac{1}{p} = \log\log x - \log\log\sqrt{x} + O\left(\frac{1}{\log x}\right) = \log 2 + O\left(\frac{1}{\log x}\right).$$

The theorem follows.

The Sieve of Eratosthenes:

- We begin by illustrating the approach with an easy consequence of Theorem 33. It should be noted that some similarities exist with the argument below and the sieve proof given for Theorem 15.

- **Theorem 39.** $\pi(x) = o(x)$.

- **Proof.** The number of positive integers $\le x$ divisible by a product of primes $p_1p_2\dots p_r$ is $[x/(p_1p_2\dots p_r)]$. The inclusion-exclusion principal implies that the number of positive integers $n \le x$ with each prime factor of n being greater than z is

$$[x] - \sum_{p\le z}\left[\frac{x}{p}\right] + \sum_{p_1<p_2\le z}\left[\frac{x}{p_1p_2}\right] - \sum_{p_1<p_2<p_3\le z}\left[\frac{x}{p_1p_2p_3}\right] + \cdots$$

$$= x - \sum_{p\le z}\frac{x}{p} + \sum_{p_1<p_2\le z}\frac{x}{p_1p_2} - \cdots + O\left(1 + \sum_{p\le z} 1 + \sum_{p_1<p_2\le z} 1 + \cdots\right)$$

$$= x\prod_{p\le z}\left(1-\frac{1}{p}\right) + O\left(\binom{\pi(z)}{0} + \binom{\pi(z)}{1} + \binom{\pi(z)}{2} + \cdots\right).$$

The big-oh term is $\ll 2^{\pi(z)} \ll 2^z$. We take $z = \log x$ and use Theorem 37 (iii) to deduce that

$$x\prod_{p\le z}\left(1-\frac{1}{p}\right) \ll \frac{x}{\log\log x}.$$

Also, this choice of z gives $2^z = x^{\log 2}$. We obtain that the number of positive integers $n \le x$ with each prime factor of n being greater than $\log x$ is $o(x)$. This accounts for all the primes $\le x$ except those which are $\le \log x$. There are clearly $o(x)$ such primes and the result follows.

- A closer look at the argument. We estimated $\pi(x)$ using the inequality

$$\pi(x) \le z + A(z,x) \qquad \text{where} \qquad A(z,x) = |\{n \le x : p|n \implies p > z\}|$$

(so that $A(z,x)$ denotes the number of positive integers $\le x$ having each of its prime divisors $> z$). We used that

$$A(z,x) = [x] - \sum_{p \le z} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le z} \left[\frac{x}{p_1 p_2}\right] - \sum_{p_1 < p_2 < p_3 \le z} \left[\frac{x}{p_1 p_2 p_3}\right] + \cdots .$$

This last identity can be justified as follows. For n a positive integer, define

$$\alpha(n) = 1 - \sum_{\substack{p \le z \\ p|n}} 1 + \sum_{\substack{p_1 < p_2 \le z \\ p_1 p_2 | n}} 1 - \sum_{\substack{p_1 < p_2 < p_3 \le z \\ p_1 p_2 p_3 | n}} 1 + \cdots .$$

Write n in the form $n = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r} m$ where r is a non-negative integer, $q_1, \ldots, q_r$ are distinct primes $\le z$, $m, e_1, \ldots, e_r$ are positive integers, and every prime divisor of m is $> z$. If $r = 0$, then clearly $\alpha(n) = 1$. If $r > 0$, then

$$\alpha(n) = 1 - \binom{r}{1} + \binom{r}{2} - \cdots \pm \binom{r}{r} = (1-1)^r = 0.$$

Thus, we deduce that

$$\alpha(n) = \begin{cases} 1 & \text{if every prime divisor of } n \text{ is } > z \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$\begin{aligned} A(z,x) &= \sum_{n \le x} \alpha(n) = \sum_{n \le x} \Bigg(1 - \sum_{\substack{p \le z \\ p|n}} 1 + \sum_{\substack{p_1 < p_2 \le z \\ p_1 p_2 | n}} 1 - \cdots \Bigg) \\ &= \sum_{n \le x} 1 - \sum_{p \le z} \sum_{\substack{n \le x \\ p|n}} 1 + \sum_{p_1 < p_2 \le z} \sum_{\substack{n \le x \\ p_1 p_2 | n}} 1 - \cdots \\ &= [x] - \sum_{p \le z} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le z} \left[\frac{x}{p_1 p_2}\right] - \sum_{p_1 < p_2 < p_3 \le z} \left[\frac{x}{p_1 p_2 p_3}\right] + \cdots . \end{aligned}$$

We will modify our choice for $\alpha(n)$ slightly for other applications. The basic approach we used to estimate $A(z,x)$ is called the sieve of Eratosthenes. We give two more examples.

- **Theorem 40.** *The number of squarefree numbers $\le x$ is asymptotic to $(6/\pi^2)x$.*
- **Proof.** We make use of the identity

$$(*) \qquad \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2}.$$

One can obtain $(*)$ from

$$\prod_p \left(1-\frac{1}{p^2}\right)^{-1} = \prod_p \left(1+\frac{1}{p^2}+\frac{1}{p^4}+\cdots\right) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}.$$

Denote by $A_1(z,x)$ the number of $n \le x$ that are not divisible by p^2 for every $p \le z$. Let $A_2(z,x)$ denote the number of such n that are not squarefree. In other words,

$$A_1(z,x) = |\{n \le x : p^2 | n \implies p > z\}|$$

and

$$A_2(z,x) = |\{n \le x : p^2 | n \implies p > z, \exists p \text{ such that } p^2 | n\}|.$$

By the sieve of Eratosthenes,

$$\begin{aligned} A_1(z,x) &= \sum_{n\le x}\Bigg(1 - \sum_{\substack{p\le z\\ p^2|n}} 1 + \sum_{\substack{p_1<p_2\le z\\ p_1^2p_2^2|n}} 1 - \cdots\Bigg) \\ &= [x] - \sum_{p\le z}\left[\frac{x}{p^2}\right] + \sum_{p_1<p_2\le z}\left[\frac{x}{p_1^2p_2^2}\right] - \cdots = x\prod_{p\le z}\left(1-\frac{1}{p^2}\right) + O\big(2^{\pi(z)}\big). \end{aligned}$$

Taking $z = \log x$, we obtain

$$A_1(z,x) = x\prod_{p\le \log x}\left(1-\frac{1}{p^2}\right) + O\big(2^{\log x}\big) = x\prod_{p\le \log x}\left(1-\frac{1}{p^2}\right) + o\big(x\big).$$

Thus, $A_1(z,x) \sim (6/\pi^2)x$ (with $z = \log x$). Since the number of squarefree numbers $\le x$ is $A_1(z,x) - A_2(z,x)$, it suffices to show $A_2(z,x) = o(x)$. We use that

$$A_2(z,x) \le \sum_{n\le x}\sum_{\substack{p>z\\ p^2|n}} 1 = \sum_{p>z}\sum_{\substack{n\le x\\ p^2|n}} 1 = \sum_{p>z}\left[\frac{x}{p^2}\right] \le x\Bigg(\sum_{p>z}\frac{1}{p^2}\Bigg).$$

The series $\sum_p \frac{1}{p^2}$ converges by comparison with $\sum_{n=1}^{\infty}\frac{1}{n^2}$. Since $z = \log x$ and $\sum_{p>z}\frac{1}{p^2}$ is the tail end of a convergent series, we deduce that $\sum_{p>z}\frac{1}{p^2} = o(1)$. It follows that $A_2(z,x) = o(x)$, completing the proof.

- **Comment:** Let $\zeta(k) = \sum_{k=1}^{\infty}\frac{1}{n^k}$. An argument similar to the above shows that for every integer $k > 1$, the number of k-free numbers $\le x$ is asymptotic to $x/\zeta(k)$.

- **Theorem 41.** *Let T be a set of positive integers with the property that for every odd prime p, every sufficiently large multiple of p is in T. In other words, T is such that if p is* *an odd prime, then there is a $k_0(p)$ for which $kp \in T$ for every positive integer $k \geq k_0(p)$. Define $T(x)$ as the number of elements of T that are $\leq x$. Then $T(x) \sim x$.*

• **Comments.** It will follow from the proof that the existence of $k_0(p)$ only needs to hold for a set of primes $\mathcal{P}$ having the property that $\sum_{p \in \mathcal{P}} (1/p)$ diverges. Theorem 41 is connected to Fermat's Last Theorem. Explain this connection.

• **Proof.** Fix $\varepsilon > 0$. It suffices to show that there is an $x_0(\varepsilon)$ such that if $x \geq x_0(\varepsilon)$, then

$$1 - \varepsilon \leq \frac{T(x)}{x} \leq 1.$$

The upper bound is obvious. For $z > 0$, define $K = K(z) = \max\{k_0(p) : 2 < p \leq z\}$. Then for each prime $p \leq z$ and each integer $k \geq K$, we have $kp \in T$. Let $S = \{n \in \mathbb{Z}^+ : n \notin T\}$, and define $S(x) = |\{n \leq x : n \in S\}|$. Thus,

$$S(x) = [x] - T(x).$$

For each $z > 0$ and each odd prime $p \leq z$, there are $\leq K = K(z)$ multiples of p in S. The remaining elements of S are not multiples of any odd prime $p \leq z$. In other words, the remaining elements of S have all their odd prime factors $> z$. Thus,

$$S(x) \leq \sum_{p \leq z} K + A(z,x) \quad \text{where} \quad A(z,x) = |\{n \leq x : p|n \implies p = 2 \text{ or } p > z\}|.$$

Now,

$$\begin{aligned} A(z,x) &= \sum_{n \leq x} \Bigg(1 - \sum_{\substack{2<p\leq z \\ p|n}} 1 + \sum_{\substack{2<p_1<p_2\leq z \\ p_1p_2|n}} 1 - \cdots \Bigg) = [x] - \sum_{2<p\leq z} \left[\frac{x}{p}\right] + \sum_{2<p_1<p_2\leq z} \left[\frac{x}{p_1p_2}\right] - \cdots \\ &= x \prod_{2<p\leq z} \left(1 - \frac{1}{p}\right) + O\big(2^{\pi(z)}\big) = 2x \prod_{p \leq z} \left(1 - \frac{1}{p}\right) + O\big(2^z\big). \end{aligned}$$

Taking $z = e^{4/\varepsilon}$ and using the lemma to Theorem 28, we deduce that

$$S(x) \leq K\pi(z) + A(z,x) \leq Kz + \frac{2x}{\log z} + O\big(2^z\big) \leq Ke^{4/\varepsilon} + \frac{\varepsilon}{2}x + O\big(2^{e^{4/\varepsilon}}\big) = \frac{\varepsilon}{2}x + O(1)$$

where the implied constant depends on ε and K (but note that K only depends on ε). For x sufficiently large, we obtain $S(x) \leq \varepsilon x - 1$ so that

$$T(x) = [x] - S(x) \geq x - 1 - (\varepsilon x - 1) = (1 - \varepsilon)x.$$

This completes the proof.

Homework:

(1) (a) Let $\mathcal{P}$ be a set of primes for which $\sum_{p\in\mathcal{P}}(1/p)$ diverges. Explain why $\sum_{p\in\mathcal{P}}\log\left(1-\frac{1}{p}\right)$ diverges.

(b) Given the set $\mathcal{P}$ in (a), explain why $\lim_{z\to\infty}\prod_{p\le z, p\in\mathcal{P}}\left(1-\frac{1}{p}\right)=0$.

(c) Justify the first comment made after the statement of Theorem 41.

(2) (a) For $z>1$, define

$$\alpha(n)=1-\sum_{\substack{p\le z\\ p\equiv 3 \pmod 4\\ p|n}}1+\sum_{\substack{p_1<p_2\le z\\ p_1\equiv p_2\equiv 3 \pmod 4\\ p_1p_2|n}}1-\sum_{\substack{p_1<p_2<p_3\le z\\ p_1\equiv p_2\equiv p_3\equiv 3 \pmod 4\\ p_1p_2p_3|n}}1+\cdots.$$

Prove that $\alpha(n)=1$ if $x^2+1\equiv 0 \pmod n$ has a solution and that $\alpha(n)\ge 0$ for all positive integers n.

(b) Use a sieve argument to show that for almost all positive integers n, $x^2+1\equiv 0 \pmod n$ does not have a solution. In other words, show that the number of $n\le x$ for which $x^2+1\equiv 0 \pmod n$ has a solution is $o(x)$.

The Pure Brun Sieve:

- The idea. The sieve of Eratosthenes was based on estimating $\sum_{n\le x}\alpha(n)$ where $\alpha(n)$ is something like (depending on the application)

$$\alpha(n)=1-\sum_{\substack{p\le z\\ p|n}}1+\sum_{\substack{p_1<p_2\le z\\ p_1p_2|n}}1-\sum_{\substack{p_1<p_2<p_3\le z\\ p_1p_2p_3|n}}1+\cdots.$$

One major goal of sieve methods is to take z as large as possible without causing the error terms that arise to exceed what one expects the main term to be. In the sieve of Eratosthenes, we took $z=\log x$ which caused the error term $O(2^z)$ not to be too large. The choice of $\alpha(n)$ above has the property that

$$\alpha(n)=\begin{cases}1 & \text{if every prime divisor of } n \text{ is } >z\\ 0 & \text{otherwise}\end{cases}$$

so that $|\{n\le x: p|n \implies p>z\}|=\sum_{n\le x}\alpha(n)$. We fix a positive integer k and define a new quantity

$$\alpha'(n)=1-\sum_{\substack{p\le z\\ p|n}}1+\sum_{\substack{p_1<p_2\le z\\ p_1p_2|n}}1-\cdots+\sum_{\substack{p_1<p_2<\cdots<p_{2k}\le z\\ p_1p_2\cdots p_{2k}|n}}1.$$

We will show that

$$(*)\qquad |\{n\le x: p|n \implies p>z\}|\le\sum_{n\le x}\alpha'(n).$$

The advantage of using $\alpha'(n)$ over $\alpha(n)$ can be seen as follows. Recall that in using $\alpha(n)$, we were led to considering sums of expressions of the form $[x/(p_1p_2\cdots p_r)]$ where the p_j denoted primes satisfying $p_1 < p_2 < \cdots < p_r \le z$. In that approach, we then replaced this expression with $x/(p_1p_2\cdots p_r) + O(1)$. We can see immediately that this is too wasteful if r (and, hence, z) is large. For example, if $z = (\log x)^2$ and $r = \pi(z)$ are large, then $p_1p_2\cdots p_r = \prod_{p\le z} p \ge e^{z/2} = x^{(\log x)/2}$ is so large that $[x/(p_1p_2\cdots p_r)] = 0$ and $[x/(p_1p_2\cdots p_r)]$ is very close to the value of $x/(p_1p_2\cdots p_r)$. Our method used an error of $O(1)$ when in fact the true error was much smaller. By limiting the number of primes one considers as in the definition of $\alpha'(n)$, one can better control the lost made by omitting the greatest integer function. This in turn allows us to choose z larger than before. In particular, in the application we describe shortly, we will take $z = x^{1/(24\log\log x)}$.

• **Comments:** A lower bound similar to the upper bound given in $(*)$ can be obtained by considering $2k+1$ instead of $2k$ primes in the definition of $\alpha'(n)$. Further sieve methods, due independently to Brun and Selberg, allow one to take z even larger than that mentioned above. Typically, one can $z = x^c$ where c is a positive constant depending on the application.

• A property of $\alpha'(n)$. We show that $\alpha'(n) = 1$ if every prime divisor of n is $> z$ and that $\alpha'(n) \ge 0$ for all n. Observe that $(*)$ follows as a consequence. The first part is obvious for if every prime factor of n is $> z$, then all the sums in the definition of $\alpha'(n)$ are empty and only the term 1 is non-zero in this definition. Now, suppose $n = q_1^{e_1}q_2^{e_2}\cdots q_r^{e_r}m$ where the q_j are distinct primes $\le z$, each of $r, e_1, \dots, e_r$ are positive integers, and every prime factor of m is $> z$. It follows that

$$(**)\qquad \alpha'(n) = 1 - \binom{r}{1} + \binom{r}{2} - \cdots + \binom{r}{2k},$$

where we interpret $\binom{a}{b}$ as 0 is $b > a$. To show that $\alpha'(n) \ge 0$, consider three cases: (i) $r \le 2k$, (ii) $2k < r \le 4k$, and (iii) $r > 4k$. Case (i) is dealt with by using $(1-1)^r = 0$ to show $\alpha'(n) = 0$. For Case (ii), use $(1-1)^r = 0$ to obtain

$$\begin{aligned}\alpha'(n) &= \binom{r}{2k+1} - \binom{r}{2k+2} + \cdots \pm \binom{r}{r}\\ &\ge \left(\binom{r}{2k+1} - \binom{r}{2k+2}\right) + \left(\binom{r}{2k+3} - \binom{r}{2k+4}\right) + \cdots \ge 0.\end{aligned}$$

For Case (iii), use $(**)$ directly to show that $\alpha'(n) \ge 1$ (by again grouping the binomial coefficients in pairs).

• An estimate concerning twin primes. A twin prime is a prime p for which $p-2$ or $p+2$ is also prime. Thus, 3, 5, 7, 11, 13, 17, 19, 29, and 31 are all twin primes. We denote the number of twin primes $\le x$ by $\pi_2(x)$. We will show

Theorem 42. $\pi_2(x) \ll \dfrac{x}{\log^2 x}(\log\log x)^2$.

More generally, we denote by $\pi_a(x)$ the number of primes $p \le x$ for which $p-a$ or $p+a$ is also prime. We prove our next theorem from which Theorem 42 follows.

Theorem 43. *Let a be a positive integer. Then $\pi_a(x) \ll \dfrac{x}{\log^2 x}(\log\log x)^2$ where the implied constant depends on a.*

- **Proof.** We define

$$A'(z,x) = |\{n \le x : p|n(n+a) \implies p > z\}|.$$

Observe that for z sufficiently large (eg., $z \ge 2a+2$ so that $\pi(z)+a \le z$), we have $\pi_a(x) \le 2A'(z,x)+z$. We seek a good estimate for $A'(z,x)$. We use that

$$\begin{aligned} A'(z,x) &\le \sum_{n\le x} \alpha'(n(n+a)) \\ &= \sum_{n\le x} 1 - \sum_{p\le z} \sum_{\substack{n\le x \\ p|n(n+a)}} 1 + \sum_{p_1<p_2\le z} \sum_{\substack{n\le x \\ p_1p_2|n(n+a)}} 1 \\ &\quad - \cdots + \sum_{p_1<p_2<\cdots<p_{2k}\le z} \sum_{\substack{n\le x \\ p_1p_2\cdots p_{2k}|n(n+a)}} 1. \end{aligned}$$

We fix momentarily $z \ge a$ so that if $p|a$, then $p \le z$. For a given $p \le z$, we consider two possibilities, $p|a$ and $p \nmid a$. If $p|a$, then the number of $n \le x$ for which $p|n(n+a)$ is $[x/p]$, which is within 1 of x/p. If $p \nmid a$, then the number of $n \le x$ for which $p|n(n+a)$ is within 2 of $2x/p$. In general, if $p_1,\dots,p_u$ are distinct primes dividing a and $p_{u+1},\dots,p_{u+v}$ are distinct primes not dividing a, then the number of $n \le x$ for which $n(n+a)$ is divisible by $p_1p_2\cdots p_{u+v}$ is within 2^v of $2^vx/\big(p_1p_2\cdots p_{u+v}\big)$ (this can be seen by using the Chinese Remainder Theorem and considering the number of such n in a complete system of residues modulo $p_1p_2\cdots p_{u+v}$). It follows that

$$\begin{aligned} A'(z,x) &\le x - \sum_{\substack{p\le z \\ p|a}} \frac{x}{p} - \sum_{\substack{p\le z \\ p\nmid a}} \frac{2x}{p} + \sum_{\substack{p_1<p_2\le z \\ p_1p_2|a}} \frac{x}{p_1p_2} \\ &\quad + \sum_{\substack{p_1<p_2\le z \\ p_1|a,p_2\nmid a}} \frac{2x}{p_1p_2} + \sum_{\substack{p_1<p_2\le z \\ p_1\nmid a,p_2|a}} \frac{2x}{p_1p_2} + \sum_{\substack{p_1<p_2\le z \\ p_1\nmid a,p_2\nmid a}} \frac{4x}{p_1p_2} \\ &\quad - \cdots + \sum_{\substack{p_1<p_2<\cdots<p_{2k}\le z \\ p_1\nmid a,\dots,p_{2k}\nmid a}} \frac{2^{2k}x}{p_1\cdots p_{2k}} + E_1 \\ &= \prod_{p|a}\left(1-\frac{1}{p}\right) \prod_{\substack{p\le z \\ p\nmid a}} \left(1-\frac{2}{p}\right) x + E_1 + E_2, \end{aligned}$$

where

$$E_1 \leq 1 + 2\binom{\pi(z)}{1} + 4\binom{\pi(z)}{2} + \cdots + 2^{2k}\binom{\pi(z)}{2k}$$
$$\leq \pi(z)^{2k}\left(1 + 2 + \frac{2^2}{2!} + \cdots + \frac{2^{2k}}{(2k)!}\right) \leq e^2\pi(z)^{2k}$$

and

$$E_2 \leq \sum_{p_1<p_2<\cdots<p_{2k+1}\leq z} \frac{2^{2k+1}x}{p_1p_2\cdots p_{2k+1}} + \sum_{p_1<p_2<\cdots<p_{2k+2}\leq z} \frac{2^{2k+2}x}{p_1p_2\cdots p_{2k+2}} + \cdots$$
$$\leq x\sum_{u=2k+1}^{\infty} \frac{1}{u!}\left(\sum_{p\leq z}\frac{2}{p}\right)^u \leq x\sum_{u=2k+1}^{\infty}\frac{1}{u!}\left(2\log\log z + 2C_1\right)^u,$$

where C_1 is some appropriate constant. Using $e^u = \sum_{j=0}^{\infty} u^j/j! \geq u^u/u!$ and choosing $k = [6\log\log z]$, we obtain

$$E_2 \leq x\sum_{u=2k+1}^{\infty}\left(\frac{2e\log\log z + 2eC_1}{u}\right)^u \leq x\sum_{u=2k+1}^{\infty}\left(\frac{1}{2}\right)^u = \frac{x}{2^{2k}} < \frac{x}{(\log z)^6}$$

for z sufficiently large. We also have

$$E_1 \leq e^2\pi(z)^{2k} \leq z^{12\log\log z}$$

for z sufficiently large. We now choose $z = x^{1/(24\log\log x)}$ and consider x sufficiently large to deduce that

$$A'(z,x) \leq \prod_{p|a}\left(1-\frac{1}{p}\right)\prod_{\substack{p\leq z\\ p\nmid a}}\left(1-\frac{2}{p}\right)x + E,$$

where $|E| \leq x/(\log x)^5$. Observe that, for some constants C_2 and C_3 depending on a,

$$\prod_{p|a}\left(1-\frac{1}{p}\right)\prod_{\substack{p\leq z\\ p\nmid a}}\left(1-\frac{2}{p}\right)x \leq C_2x\left(\prod_{p\leq z}\left(1-\frac{1}{p}\right)\right)^2 \leq C_3\frac{x}{(\log x)^2}(\log\log x)^2.$$

Theorem 43 follows.

- Brun's Theorem. Brun introduced his pure sieve and used it to establish

Theorem 44. $\displaystyle\sum_{p \text{ a twin prime}} (1/p)$ *converges.*

- **Proof.** We use Riemann-Stieltjes integrals to obtain

$$\sum_{\substack{p\leq x\\ p \text{ a twin prime}}} \frac{1}{p} = \int_1^x \frac{1}{t}\,d\pi_2(t) = \frac{\pi_2(x)}{x} + \int_2^x \frac{\pi_2(t)}{t^2}\,dt.$$

Clearly, $\pi_2(x)/x \le 1$. Also, Theorem 43 implies

$$\frac{\pi_2(t)}{t^2} \ll \frac{(\log\log t)^2}{t(\log t)^2} \ll \frac{1}{t(\log t)^{3/2}}$$

so that

$$\int_2^x \frac{\pi_2(t)}{t^2}\,dt \ll \int_2^x \frac{1}{t(\log t)^{3/2}}\,dt \ll 1.$$

Thus, $\displaystyle\sum_{p \text{ a twin prime}} \frac{1}{p}$ is a bounded infinite series with positive terms. The theorem follows.

Homework:

(1) Let p_n denote the nth prime.

(a) Explain why the Prime Number Theorem implies that $\limsup_{n\to\infty}(p_{n+1} - p_n) = \infty$.

(b) Use Theorem 43 to prove that for every positive integer k,

$$\limsup_{n\to\infty} \big(\min\{p_{n+1} - p_n, p_{n+2} - p_{n+1}, \dots, p_{n+k} - p_{n+k-1}\}\big) = \infty.$$

(Note that this would follow from part (a) if "min" were replaced by "max"; the problem is to figure out how to handle the "min" situation.)