Number Theory

Naoki Sato <sato@artofproblemsolving.com>

0 Preface

This set of notes on number theory was originally written in 1995 for students at the IMO level. It covers the basic background material that an IMO student should be familiar with. This text is meant to be a reference, and not a replacement but rather a supplement to a number theory textbook; several are given at the back. Proofs are given when appropriate, or when they illustrate some insight or important idea. The problems are culled from various sources, many from actual contests and olympiads, and in general are very difficult. The author welcomes any corrections or suggestions.

1 Divisibility

For integers a and b, we say that a **divides** b, or that a is a **divisor** (or **factor**) of b, or that b is a **multiple** of a, if there exists an integer c such that $b = ca$, and we denote this by $a \mid b$. Otherwise, a does not divide b, and we denote this by $a \nmid b$. A positive integer p is a **prime** if the only divisors of p are 1 and p. If $p^k \mid a$ and $p^{k+1} \nmid a$ where p is a prime, i.e. p^k is the highest power of p dividing a, then we denote this by $p^k \| a$.

Useful Facts

- If $a, b > 0$, and $a \mid b$, then $a \leq b$.
- If $a \mid b_1$, $a \mid b_2$, $\ldots$, $a \mid b_n$, then for any integers c_1, c_2, $\ldots$, c_n,

$$a \mid \sum_{i=1}^{n} b_i c_i.$$

Theorem 1.1. *The Division Algorithm.* For any positive integer a and integer b, there exist unique integers q and r such that $b = qa + r$ and $0 \leq r < a$, with $r = 0$ iff $a \mid b$.

Theorem 1.2. *The Fundamental Theorem of Arithmetic.* Every integer greater than 1 can be written uniquely in the form

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where the p_i are distinct primes and the e_i are positive integers.

Theorem 1.3. (Euclid) There exist an infinite number of primes.

Proof. Suppose that there are a finite number of primes, say p_1, p_2, ..., p_n. Let $N = p_1 p_2 \cdots p_n + 1$. By the fundamental theorem of arithmetic, N is divisible by some prime p. This prime p must be among the p_i, since by assumption these are all the primes, but N is seen not to be divisible by any of the p_i, contradiction.

Example 1.1. Let x and y be integers. Prove that $2x + 3y$ is divisible by 17 iff $9x + 5y$ is divisible by 17.

Solution. $17 \mid (2x + 3y) \Rightarrow 17 \mid [13(2x + 3y)]$, or $17 \mid (26x + 39y) \Rightarrow 17 \mid (9x + 5y)$, and conversely, $17 \mid (9x + 5y) \Rightarrow 17 \mid [4(9x + 5y)]$, or $17 \mid (36x + 20y) \Rightarrow 17 \mid (2x + 3y)$.

Example 1.2. Find all positive integers d such that d divides both n^2+1 and $(n + 1)^2 + 1$ for some integer n.

Solution. Let $d \mid (n^2 + 1)$ and $d \mid [(n + 1)^2 + 1]$, or $d \mid (n^2 + 2n + 2)$. Then $d \mid [(n^2 + 2n + 2) - (n^2 + 1)]$, or $d \mid (2n + 1) \Rightarrow d \mid (4n^2 + 4n + 1)$, so $d \mid [4(n^2+2n+2)-(4n^2+4n+1)]$, or $d \mid (4n+7)$. Then $d \mid [(4n+7)-2(2n+1)]$, or $d \mid 5$, so d can only be 1 or 5. Taking $n = 2$ shows that both of these values are achieved.

Example 1.3. Suppose that a_1, a_2, ..., a_{2n} are distinct integers such that the equation

$$(x - a_1)(x - a_2) \cdots (x - a_{2n}) - (-1)^n (n!)^2 = 0$$

has an integer solution r. Show that

$$r = \frac{a_1 + a_2 + \cdots + a_{2n}}{2n}.$$

(1984 IMO Short List)

Solution. Clearly, $r \neq a_i$ for all i, and the $r - a_i$ are $2n$ distinct integers, so

$$|(r - a_1)(r - a_2) \cdots (r - a_{2n})| \geq |(1)(2) \cdots (n)(-1)(-2) \cdots (-n)| = (n!)^2,$$

with equality iff

$$\{r - a_1, r - a_2, \ldots, r - a_{2n}\} = \{1, 2, \ldots, n, -1, -2, \ldots, -n\}.$$

Therefore, this must be the case, so

$$\begin{aligned} &(r - a_1) + (r - a_2) + \cdots + (r - a_{2n}) \\ &= 2nr - (a_1 + a_2 + \cdots + a_{2n}) \\ &= 1 + 2 + \cdots + n + (-1) + (-2) + \cdots + (-n) = 0 \\ \Rightarrow\ r &= \frac{a_1 + a_2 + \cdots + a_{2n}}{2n}. \end{aligned}$$

Example 1.4. Let $0 < a_1 < a_2 < \cdots < a_{mn+1}$ be $mn+1$ integers. Prove that you can select either $m+1$ of them no one of which divides any other, or $n+1$ of them each dividing the following one.

(1966 Putnam Mathematical Competition)

Solution. For each i, $1 \leq i \leq mn+1$, let n_i be the length of the longest sequence starting with a_i and each dividing the following one, among the integers a_i, a_{i+1}, ..., a_{mn+1}. If some n_i is greater than n then the problem is solved. Otherwise, by the pigeonhole principle, there are at least $m+1$ values of n_i that are equal. Then, the integers a_i corresponding to these n_i cannot divide each other.

Useful Facts

- *Bertrand's Postulate.* For every positive integer n, there exists a prime p such that $n \leq p \leq 2n$.
- *Gauss's Lemma.* If a polynomial with integer coefficients factors into two polynomials with rational coefficients, then it factors into two polynomials with integer coefficients.

Problems

1. Let a and b be positive integers such that $a \mid b^2$, $b^2 \mid a^3$, $a^3 \mid b^4$, $b^4 \mid a^5$, ... Prove that $a = b$.
2. Let a, b, and c denote three distinct integers, and let P denote a polynomial having all integral coefficients. Show that it is impossible that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

   (1974 USAMO)

3. Show that if a and b are positive integers, then

$$\left(a+\frac{1}{2}\right)^n+\left(b+\frac{1}{2}\right)^n$$

is an integer for only finitely many positive integers n.

(*A Problem Seminar*, D.J. Newman)

4. For a positive integer n, let $r(n)$ denote the sum of the remainders when n is divided by 1, 2, ..., n respectively. Prove that $r(k)=r(k-1)$ for infinitely many positive integers k.

(1981 Kürschák Competition)

5. Prove that for all positive integers n,

$$0<\sum_{k=1}^{n}\frac{g(k)}{k}-\frac{2n}{3}<\frac{2}{3},$$

where $g(k)$ denotes the greatest odd divisor of k.

(1973 Austrian Mathematics Olympiad)

6. Let d be a positive integer, and let S be the set of all positive integers of the form x^2+dy^2, where x and y are non-negative integers.

   (a) Prove that if $a\in S$ and $b\in S$, then $ab\in S$.

   (b) Prove that if $a\in S$ and $p\in S$, such that p is a prime and $p\mid a$, then $a/p\in S$.

   (c) Assume that the equation $x^2+dy^2=p$ has a solution in non-negative integers x and y, where p is a given prime. Show that if $d\geq 2$, then the solution is unique, and if $d=1$, then there are exactly two solutions.

2 GCD and LCM

The **greatest common divisor** of two positive integers a and b is the greatest positive integer that divides both a and b, which we denote by $\gcd(a,b)$, and similarly, the **lowest common multiple** of a and b is the least positive

integer that is a multiple of both a and b, which we denote by $\text{lcm}(a, b)$. We say that a and b are **relatively prime** if $\gcd(a, b) = 1$. For integers a_1, a_2, $\ldots$, a_n, $\gcd(a_1, a_2, \ldots, a_n)$ is the greatest positive integer that divides all of a_1, a_2, $\ldots$, a_n, and $\text{lcm}(a_1, a_2, \ldots, a_n)$ is defined similarly.

Useful Facts

- For all a, b, $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.
- For all a, b, and m, $\gcd(ma, mb) = m \gcd(a, b)$ and $\text{lcm}(ma, mb) = m\text{lcm}(a, b)$.
- If $d \mid \gcd(a, b)$, then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\gcd(a, b)}{d}.$$

  In particular, if $d = \gcd(a, b)$, then $\gcd(a/d, b/d) = 1$; that is, a/d and b/d are relatively prime.
- If $a \mid bc$ and $\gcd(a, c) = 1$, then $a \mid b$.
- For positive integers a and b, if d is a positive integer such that $d \mid a$, $d \mid b$, and for any d', $d' \mid a$ and $d' \mid b$ implies that $d' \mid d$, then $d = \gcd(a, b)$. This is merely the assertion that any common divisor of a and b divides $\gcd(a, b)$.
- If $a_1 a_2 \cdots a_n$ is a perfect k^{th} power and the a_i are pairwise relatively prime, then each a_i is a perfect k^{th} power.
- Any two consecutive integers are relatively prime.

Example 2.1. Show that for any positive integer N, there exists a multiple of N that consists only of 1s and 0s. Furthermore, show that if N is relatively prime to 10, then there exists a multiple that consists only of 1s.

Solution. Consider the $N + 1$ integers 1, 11, 111, $\ldots$, 111...1 ($N + 1$ 1s). When divided by N, they leave $N + 1$ remainders. By the pigeonhole principle, two of these remainders are equal, so the difference in the corresponding integers, an integer of the form 111...000, is divisible by N. If N is relatively prime to 10, then we may divide out all powers of 10, to obtain an integer of the form 111...1 that remains divisible by N.

Theorem 2.1. For any positive integers a and b, there exist integers x and y such that $ax + by = \gcd(a, b)$. Furthermore, as x and y vary over all integers, $ax + by$ attains all multiples and only multiples of $\gcd(a, b)$.

Proof. Let S be the set of all integers of the form $ax+by$, and let d be the least positive element of S. By the division algorithm, there exist integers q and r such that $a = qd + r$, $0 \leq r < d$. Then $r = a - qd = a - q(ax + by) = (1 - qx)a - (qy)b$, so r is also in S. But $r < d$, so $r = 0 \Rightarrow d \mid a$, and similarly, $d \mid b$, so $d \mid \gcd(a, b)$. However, $\gcd(a, b)$ divides all elements of S, so in particular $\gcd(a, b) \mid d \Rightarrow d = \gcd(a, b)$. The second part of the theorem follows.

Corollary 2.2. The positive integers a and b are relatively prime iff there exist integers x and y such that $ax + by = 1$.

Corollary 2.3. For any positive integers a_1, a_2, ..., a_n, there exist integers $x_1, x_2, \ldots, x_n$, such that $a_1x_1+a_2x_2+\cdots+a_nx_n = \gcd(a_1, a_2, \ldots, a_n)$.

Corollary 2.4. Let a and b be positive integers, and let n be an integer. Then the equation

$$ax + by = n$$

has a solution in integers x and y iff $\gcd(a, b) \mid n$. If this is the case, then all solutions are of the form

$$(x, y) = \left(x_0 + t \cdot \frac{b}{d} \ , \ y_0 - t \cdot \frac{a}{d} \right),$$

where $d = \gcd(a, b)$, (x_0, y_0) is a specific solution of $ax + by = n$, and t is an integer.

Proof. The first part follows from Theorem 2.1. For the second part, as stated, let $d = \gcd(a, b)$, and let (x_0, y_0) be a specific solution of $ax + by = n$, so that $ax_0 + by_0 = n$. If $ax + by = n$, then $ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0$, or $a(x - x_0) = b(y_0 - y)$, and hence

$$(x - x_0) \cdot \frac{a}{d} = (y_0 - y) \cdot \frac{b}{d}.$$

Since a/d and b/d are relatively prime, b/d must divide $x - x_0$, and a/d must divide $y_0 - y$. Let $x - x_0 = tb/d$ and $y_0 - y = ta/d$. This gives the solutions described above.

Example 2.2. Prove that the fraction

$$\frac{21n+4}{14n+3}$$

is irreducible for every positive integer n. (1959 IMO)

Solution. For all n, $3(14n+3)-2(21n+4)=1$, so the numerator and denominator are relatively prime.

Example 2.3. For all positive integers n, let $T_n = 2^{2^n}+1$. Show that if $m \neq n$, then T_m and T_n are relatively prime.

Solution. We have that

$$\begin{aligned} T_n - 2 &= 2^{2^n} - 1 = 2^{2^{n-1}\cdot 2} - 1 \\ &= (T_{n-1}-1)^2 - 1 = T_{n-1}^2 - 2T_{n-1} \\ &= T_{n-1}(T_{n-1}-2) \\ &= T_{n-1}T_{n-2}(T_{n-2}-2) \\ &= \cdots \\ &= T_{n-1}T_{n-2}\cdots T_1T_0(T_0-2) \\ &= T_{n-1}T_{n-2}\cdots T_1T_0, \end{aligned}$$

for all n. Therefore, any common divisor of T_m and T_n must divide 2. But each T_n is odd, so T_m and T_n are relatively prime.

Remark. It immediately follows from this result that there are an infinite number of primes.

The Euclidean Algorithm. By recursive use of the division algorithm, we may find the gcd of two positive integers a and b without factoring either, and the x and y in Theorem 2.1 (and so, a specific solution in Corollary 2.4). For example, for $a = 329$ and $b = 182$, we compute

$$\begin{aligned} 329 &= 1\cdot 182 + 147, \\ 182 &= 1\cdot 147 + 35, \\ 147 &= 4\cdot 35 + 7, \\ 35 &= 5\cdot 7, \end{aligned}$$

and stop when there is no remainder. The last dividend is the gcd, so in our example, gcd(329,182) = 7. Now, working through the above equations

backwards,

$$\begin{aligned} 7 &= 147 - 4 \cdot 35 = 147 - 4 \cdot (182 - 1 \cdot 147) \\ &= 5 \cdot 147 - 4 \cdot 182 = 5 \cdot (329 - 182) - 4 \cdot 182 \\ &= 5 \cdot 329 - 9 \cdot 182. \end{aligned}$$

Remark. The Euclidean algorithm also works for polynomials.

Example 2.4. Let n be a positive integer, and let S be a subset of $n+1$ elements of the set $\{1, 2, \ldots, 2n\}$. Show that

(a) There exist two elements of S that are relatively prime, and

(b) There exist two elements of S, one of which divides the other.

Solution. (a) There must be two elements of S that are consecutive, and thus, relatively prime.

(b) Consider the greatest odd factor of each of the $n + 1$ elements in S. Each is among the n odd integers 1, 3, ..., $2n - 1$. By the pigeonhole principle, two must have the same greatest odd factor, so they differ (multiplication-wise) by a power of 2, and so one divides the other.

Example 2.5. The positive integers a_1, a_2, ..., a_n are such that each is less than 1000, and $\text{lcm}(a_i, a_j) > 1000$ for all i, j, $i \neq j$. Show that

$$\sum_{i=1}^{n} \frac{1}{a_i} < 2.$$

(1951 Russian Mathematics Olympiad)

Solution. If $\frac{1000}{m+1} < a \leq \frac{1000}{m}$, then the m multiples a, $2a$, ..., ma do not exceed 1000. Let k_1 the number of a_i in the interval $(\frac{1000}{2}, 1000]$, k_2 in $(\frac{1000}{3}, \frac{1000}{2}]$, etc. Then there are $k_1 + 2k_2 + 3k_3 + \cdots$ integers, no greater than 1000, that are multiples of at least one of the a_i. But the multiples are distinct, so

$$\begin{aligned} & k_1 + 2k_2 + 3k_3 + \cdots < 1000 \\ \Rightarrow\ & 2k_1 + 3k_2 + 4k_3 + \cdots = (k_1 + 2k_2 + 3k_3 + \cdots) + (k_1 + k_2 + k_3 + \cdots) \\ & \qquad < 1000 + n \\ & \qquad < 2000. \end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{i=1}^{n} \frac{1}{a_i} &\leq k_1 \frac{2}{1000} + k_2 \frac{3}{1000} + k_3 \frac{4}{1000} + \cdots \\ &= \frac{2k_1 + 3k_2 + 4k_3 + \cdots}{1000} \\ &< 2.\end{aligned}$$

Note: It can be shown that $n \leq 500$ as follows: Consider the greatest odd divisor of a_1, a_2, $\ldots$, a_{1000}. Each must be distinct; otherwise, two differ, multiplication-wise, by a power of 2, which means one divides the other, contradiction. Also, there are only 500 odd numbers between 1 and 1000, from which the result follows. It also then follows that

$$\sum_{i=1}^{n} \frac{1}{a_i} < \frac{3}{2}.$$

Useful Facts

- *Dirichlet's Theorem.* If a and b are relatively prime positive integers, then the arithmetic sequence a, $a + b$, $a + 2b$, $\ldots$, contains infinitely many primes.

Problems

1. The symbols $(a, b, \ldots, g)$ and $[a, b, \ldots, g]$ denote the greatest common divisor and lowest common multiple, respectively of the positive integers a, b, $\ldots$, g. Prove that

$$\frac{[a,b,c]^2}{[a,b][a,c][b,c]} = \frac{(a,b,c)^2}{(a,b)(a,c)(b,c)}.$$

   (1972 USAMO)

2. Show that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ for all positive integers $a > 1$, m, n.

3. Let a, b, and c be positive integers. Show that

$$\text{lcm}(a,b,c) = \frac{abc \cdot \gcd(a,b,c)}{\gcd(a,b) \cdot \gcd(a,c) \cdot \gcd(b,c)}.$$

Express $\gcd(a,b,c)$ in terms of abc, $\text{lcm}(a,b,c)$, $\text{lcm}(a,b)$, $\text{lcm}(a,c)$, and $\text{lcm}(b,c)$. Generalize.

4. Let a, b be odd positive integers. Define the sequence (f_n) by putting $f_1 = a$, $f_2 = b$, and by letting f_n for $n \geq 3$ be the greatest odd divisor of $f_{n-1} + f_{n-2}$. Show that f_n is constant for n sufficiently large and determine the eventual value as a function of a and b.

(1993 USAMO)

5. Let $n \geq a_1 > a_2 > \cdots > a_k$ be positive integers such that $\text{lcm}(a_i, a_j) \leq n$ for all i, j. Prove that $ia_i \leq n$ for $i = 1, 2, \ldots, k$.

3 Arithmetic Functions

There are several important arithmetic functions, of which three are presented here. If the prime factorization of $n > 1$ is $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then the number of positive integers less than n, relatively prime to n, is

$$\begin{aligned}\phi(n) &= \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)n \\ &= p_1^{e_1-1}p_2^{e_2-1}\cdots p_k^{e_k-1}(p_1-1)(p_2-1)\cdots(p_k-1),\end{aligned}$$

the number of divisors of n is

$$\tau(n) = (e_1+1)(e_2+1)\cdots(e_k+1),$$

and the sum of the divisors of n is

$$\begin{aligned}\sigma(n) &= (p_1^{e_1} + p_1^{e_1-1} + \cdots + 1)(p_2^{e_2} + p_2^{e_2-1} + \cdots + 1) \\ &\quad \cdots (p_k^{e_k} + p_k^{e_k-1} + \cdots + 1) \\ &= \left(\frac{p_1^{e_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{e_2+1}-1}{p_2-1}\right)\cdots\left(\frac{p_k^{e_k+1}-1}{p_k-1}\right).\end{aligned}$$

Also, $\phi(1)$, $\tau(1)$, and $\sigma(1)$ are defined to be 1. We say that a function f is **multiplicative** if $f(mn) = f(m)f(n)$ for all relatively prime positive

integers m and n, and $f(1) = 1$ (otherwise, $f(1) = 0$, which implies that $f(n) = 0$ for all n).

Theorem 3.1. The functions ϕ, τ, and σ are multiplicative.

Hence, by taking the prime factorization and evaluating at each prime power, the formula above are found easily.

Example 3.1. Find the number of solutions in ordered pairs of positive integers (x, y) of the equation

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n},$$

where n is a positive integer.

Solution. From the given,

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n} \Leftrightarrow xy = nx + ny \Leftrightarrow (x - n)(y - n) = n^2.$$

If $n = 1$, then we immediately deduce the unique solution (2,2). For $n \geq 2$, let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the prime factorization of n. Since x, $y > n$, there is a 1-1 correspondence between the solutions in (x, y) and the factors of n^2, so the number of solutions is

$$\tau(n^2) = (2e_1 + 1)(2e_2 + 1) \cdots (2e_k + 1).$$

Example 3.2. Let n be a positive integer. Prove that

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

Solution. For a divisor d of n, let S_d be the set of all a, $1 \leq a \leq n$, such that $\gcd(a, n) = n/d$. Then S_d consists of all elements of the form $b \cdot n/d$, where $0 \leq b \leq d$, and $\gcd(b, d) = 1$, so S_d contains $\phi(d)$ elements. Also, it is clear that each integer between 1 and n belongs to a unique S_d. The result then follows from summing over all divisors d of n.

Problems

1. Let n be a positive integer. Prove that

$$\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor.$$

2. Let n be a positive integer. Prove that

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

3. Prove that if $\sigma(N) = 2N + 1$, then N is the square of an odd integer.
(1976 Putnam Mathematical Competition)

4 Modular Arithmetic

For a positive integer m and integers a and b, we say that a is **congruent** to b modulo m if $m \mid (a - b)$, and we denote this by $a \equiv b$ modulo m, or more commonly $a \equiv b \pmod{m}$. Otherwise, a is not congruent to b modulo m, and we denote this by $a \not\equiv b \pmod{m}$ (although this notation is not used often). In the above notation, m is called the **modulus**, and we consider the integers **modulo** m.

Theorem 4.1. If $a \equiv b$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Proof. If $a \equiv b$ and $c \equiv d \pmod{m}$, then there exist integers k and l such that $a = b + km$ and $c = d + lm$. Hence, $a + c = b + d + (k + l)m$, so $a + c \equiv b + d \pmod{m}$. Also,

$$\begin{aligned} ac &= bd + dkm + blm + klm^2 \\ &= bd + (dk + bl + klm)m, \end{aligned}$$

so $ac \equiv bd \pmod{m}$.

Useful Facts

- For all integers n,

$$n^2 \equiv \left\{ \begin{array}{c} 0 \\ 1 \end{array} \right\} \pmod{4} \left\{ \begin{array}{l} \text{if } n \text{ is even,} \\ \text{if } n \text{ is odd.} \end{array} \right.$$

- For all integers n,

$$n^2 \equiv \left\{ \begin{array}{c} 0 \\ 4 \\ 1 \end{array} \right\} \pmod{8} \left\{ \begin{array}{ll} \text{if } n \equiv 0 & \pmod{4}, \\ \text{if } n \equiv 2 & \pmod{4}, \\ \text{if } n \equiv 1 & \pmod{2}. \end{array} \right.$$

- If f is a polynomial with integer coefficients and $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.
- If f is a polynomial with integer coefficients of degree n, not identically zero, and p is a prime, then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions modulo p, counting multiplicity.

Example 4.1. Prove that the only solution in rational numbers of the equation

$$x^3 + 3y^3 + 9z^3 - 9xyz = 0$$

is $x = y = z = 0$.

(1983 Kürschák Competition)

Solution. Suppose that the equation has a solution in rationals, with at least one non-zero variable. Since the equation is homogeneous, we may obtain a solution in integers (x_0, y_0, z_0) by multiplying the equation by the cube of the lowest common multiple of the denominators. Taking the equation modulo 3, we obtain $x_0^3 \equiv 0 \pmod{3}$. Therefore, x_0 must be divisible by 3, say $x_0 = 3x_1$. Substituting,

$$\begin{aligned} &27x_1^3 + 3y_0^3 + 9z_0^3 - 27x_1y_0z_0 = 0 \\ \Rightarrow\ &y_0^3 + 3z_0^3 + 9x_1^3 - 9x_1y_0z_0 = 0. \end{aligned}$$

Therefore, another solution is (y_0, z_0, x_1). We may then apply this reduction recursively, to obtain $y_0 = 3y_1$, $z_0 = 3z_1$, and another solution (x_1, y_1, z_1). Hence, we may divide powers of 3 out of our integer solution an arbitrary number of times, contradiction.

Example 4.2. Does one of the first $10^8 + 1$ Fibonacci numbers terminate with 4 zeroes?

Solution. The answer is yes. Consider the sequence of pairs (F_k, F_{k+1}) modulo 10^4. Since there are only a finite number of different possible pairs (10^8 to be exact), and each pair is dependent only on the previous one, this sequence is eventually periodic. Also, by the Fibonacci relation, one can find the previous pair to a given pair, so this sequence is immediately periodic. But $F_0 \equiv 0 \pmod{10^4}$, so within 10^8 terms, another Fibonacci number divisible by 10^4 must appear.

In fact, a computer check shows that $10^4 \mid F_{7500}$, and (F_n) modulo 10^4 has period 15000, which is much smaller than the upper bound of 10^8.

If $ax \equiv 1 \pmod{m}$, then we say that x is the **inverse** of a modulo m, denoted by a^{-1}, and it is unique modulo m.

Theorem 4.2. The inverse of a modulo m exists and is unique iff a is relatively prime to m.

Proof. If $ax \equiv 1 \pmod{m}$, then $ax = 1+km$ for some $k \Rightarrow ax-km = 1$. By Corollary 2.2, a and m are relatively prime. Now, if $\gcd(a, m) = 1$, then by Corollary 2.2, there exist integers x and y such that $ax+my = 1 \Rightarrow ax = 1-my \Rightarrow ax \equiv 1 \pmod{m}$. The inverse x is unique modulo m, since if x' is also an inverse, then $ax \equiv ax' \equiv 1 \Rightarrow xax \equiv xax' \equiv x \equiv x'$.

Corollary 4.3. If p is a prime, then the inverse of a modulo p exists and is unique iff p does not divide a.

Corollary 4.4. If $ak \equiv bk \pmod{m}$ and k is relatively prime to m, then $a \equiv b \pmod{m}$.

Proof. Multiplying both sides by k^{-1}, which exists by Theorem 4.2, yields the result.

We say that a set $\{a_1, a_2, \ldots, a_m\}$ is a **complete residue system** modulo m if for all i, $0 \le i \le m-1$, there exists a unique j such that $a_j \equiv i \pmod{m}$.

Example 4.3. Find all positive integers n such that there exist complete residue systems $\{a_1, a_2, \ldots, a_n\}$ and $\{b_1, b_2, \ldots, b_n\}$ modulo n for which $\{a_1+b_1, a_2+b_2, \ldots, a_n+b_n\}$ is also a complete residue system.

Solution. The answer is all odd n. First we prove necessity.

For any complete residue system $\{a_1, a_2, \ldots, a_n\}$ modulo n, we have that $a_1 + a_2 + \cdots + a_n \equiv n(n+1)/2 \pmod{n}$. So, if all three sets are complete residue systems, then $a_1+a_2+\cdots+a_n+b_1+b_2+\cdots+b_n \equiv n^2+n \equiv 0 \pmod{n}$ and $a_1+b_1+a_2+b_2+\cdots+a_n+b_n \equiv n(n+1)/2 \pmod{n}$, so $n(n+1)/2 \equiv 0 \pmod{n}$. The quantity $n(n+1)/2$ is divisible by n iff $(n+1)/2$ is an integer, which implies that n is odd.

Now assume that n is odd. Let $a_i = b_i = i$ for all i. Then $a_i + b_i = 2i$ for all i, and n is relatively prime to 2, so by Corollary 4.4, $\{2, 4, \ldots, 2n\}$ is a complete residue system modulo n.

Theorem 4.5. *Euler's Theorem.* If a is relatively prime to m, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof. Let a_1, a_2, ..., $a_{\phi(m)}$ be the positive integers less than m that are relatively prime to m. Consider the integers aa_1, aa_2, ..., $aa_{\phi(m)}$. We claim that they are a permutation of the original $\phi(m)$ integers a_i, modulo m. For each i, aa_i is also relatively prime to m, so $aa_i \equiv a_k$ for some k. Since $aa_i \equiv aa_j \Leftrightarrow a_i \equiv a_j \pmod{m}$, each a_i gets taken to a different a_k under multiplication by a, so indeed they are permuted. Hence,

$$\begin{aligned} a_1 a_2 \cdots a_{\phi(m)} &\equiv (aa_1)(aa_2)\cdots(aa_{\phi(m)}) \\ &\equiv a^{\phi(m)} a_1 a_2 \cdots a_{\phi(m)} \\ \Rightarrow\ 1 &\equiv a^{\phi(m)} \pmod{m}. \end{aligned}$$

Remark. This gives an explicit formula for the inverse of a modulo m: $a^{-1} \equiv a^{\phi(m)-2} \pmod{m}$. Alternatively, one can use the Euclidean algorithm to find $a^{-1} \equiv x$ as in the proof of Theorem 4.2.

Corollary 4.6. *Fermat's Little Theorem (FLT).* If p is a prime, and p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.

Example 4.4. Show that if a and b are relatively prime positive integers, then there exist integers m and n such that $a^m + b^n \equiv 1 \pmod{ab}$.

Solution. Let $S = a^m + b^n$, where $m = \phi(b)$ and $n = \phi(a)$. Then by Euler's Theorem, $S \equiv b^{\phi(a)} \equiv 1 \pmod{a}$, or $S - 1 \equiv 0 \pmod{a}$, and $S \equiv a^{\phi(b)} \equiv 1 \pmod{b}$, or $S - 1 \equiv 0 \pmod{b}$. Therefore, $S - 1 \equiv 0$, or $S \equiv 1 \pmod{ab}$.

Example 4.5. For all positive integers i, let S_i be the sum of the products of 1, 2, ..., $p-1$ taken i at a time, where p is an odd prime. Show that $S_1 \equiv S_2 \equiv \cdots \equiv S_{p-2} \equiv 0 \pmod{p}$.

Solution. First, observe that

$$\begin{aligned} &(x-1)(x-2)\cdots(x-(p-1)) \\ &= x^{p-1} - S_1 x^{p-2} + S_2 x^{p-3} - \cdots - S_{p-2} x + S_{p-1}. \end{aligned}$$

This polynomial vanishes for $x = 1, 2, \ldots, p-1$. But by Fermat's Little Theorem, so does $x^{p-1} - 1$ modulo p. Taking the difference of these two polynomials, we obtain another polynomial of degree $p-2$ with $p-1$ roots modulo p, so it must be the zero polynomial, and the result follows from comparing coefficients.

Remark. We immediately have that $(p-1)! \equiv S_{p-1} \equiv -1 \pmod{p}$, which is Wilson's Theorem. Also, $x^p - x \equiv 0 \pmod{p}$ for all x, yet we cannot compare coefficients here. Why not?

Theorem 4.7. If p is a prime and n is an integer such that $p \mid (4n^2+1)$, then $p \equiv 1 \pmod{4}$.

Proof. Clearly, p cannot be 2, so we need only show that $p \not\equiv 3 \pmod{4}$. Suppose $p = 4k+3$ for some k. Let $y = 2n$, so by Fermat's Little Theorem, $y^{p-1} \equiv 1 \pmod{p}$, since p does not divide n. But, $y^2 + 1 \equiv 0$, so

$$y^{p-1} \equiv y^{4k+2} \equiv (y^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p},$$

contradiction. Therefore, $p \equiv 1 \pmod{4}$.

Remark. The same proof can be used to show that if p is a prime and $p \mid (n^2+1)$, then $p = 2$ or $p \equiv 1 \pmod{4}$.

Example 4.6. Show that there are an infinite number of primes of the form $4k+1$ and of the form $4k+3$.

Solution. Suppose that there are a finite number of primes of the form $4k+1$, say $p_1, p_2, \ldots, p_n$. Let $N = 4(p_1 p_2 \cdots p_n)^2 + 1$. By Theorem 4.7, N is only divisible by primes of the form $4k+1$, but clearly N is not divisible by any of these primes, contradiction.

Similarly, suppose that there are a finite number of primes of the form $4k+3$, say $q_1, q_2, \ldots, q_m$. Let $M = 4q_1 q_2 \cdots q_m - 1$. Then $M \equiv 3 \pmod{4}$, so M must be divisible by a prime of the form $4k+3$, but M is not divisible by any of these primes, contradiction.

Example 4.7. Show that if n is an integer greater than 1, then n does not divide $2^n - 1$.

Solution. Let p be the least prime divisor of n. Then $\gcd(n, p-1) = 1$, and by Corollary 2.2, there exist integers x and y such that $nx + (p-1)y = 1$. If $p \mid (2^n - 1)$, then $2 \equiv 2^{nx+(p-1)y} \equiv (2^n)^x (2^{p-1})^y \equiv 1 \pmod{p}$ by Fermat's Little Theorem, contradiction. Therefore, $p \nmid (2^n - 1) \Rightarrow n \nmid (2^n - 1)$.

Theorem 4.8. *Wilson's Theorem.* If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$. (See also Example 4.5.)

Proof. Consider the congruence $x^2 \equiv 1 \pmod{p}$. Then $x^2 - 1 \equiv (x-1)(x+1) \equiv 0$, so the only solutions are $x \equiv 1$ and -1. Therefore, for each i, $2 \le i \le p-2$, there exists a unique inverse $j \ne i$ of i, $2 \le j \le p-2$, modulo

p. Hence, when we group in pairs of inverses,

$$\begin{aligned}(p-1)! &\equiv 1 \cdot 2 \cdots (p-2) \cdot (p-1) \\ &\equiv 1 \cdot 1 \cdots 1 \cdot (p-1) \\ &\equiv -1 \pmod{p}.\end{aligned}$$

Example 4.8. Let $\{a_1, a_2, \ldots, a_{101}\}$ and $\{b_1, b_2, \ldots, b_{101}\}$ be complete residue systems modulo 101. Can $\{a_1b_1, a_2b_2, \ldots, a_{101}b_{101}\}$ be a complete residue system modulo 101?

Solution. The answer is no. Suppose that $\{a_1b_1, a_2b_2, \ldots, a_{101}b_{101}\}$ is a complete residue system modulo 101. Without loss of generality, assume that $a_{101} \equiv 0 \pmod{101}$. Then $b_{101} \equiv 0 \pmod{101}$, because if any other b_j was congruent to 0 modulo 101, then $a_jb_j \equiv a_{101}b_{101} \equiv 0 \pmod{101}$, contradiction. By Wilson's Theorem, $a_1a_2 \cdots a_{100} \equiv b_1b_2 \cdots b_{100} \equiv 100! \equiv -1 \pmod{101}$, so $a_1b_1a_2b_2 \cdots a_{100}b_{100} \equiv 1 \pmod{101}$. But $a_{101}b_{101} \equiv 0 \pmod{101}$, so $a_1b_1a_2b_2 \cdots a_{100}b_{100} \equiv 100! \equiv -1 \pmod{101}$, contradiction.

Theorem 4.9. If p is a prime, then the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution iff $p = 2$ or $p \equiv 1 \pmod{4}$. (Compare to Theorem 7.1)

Proof. If $p = 2$, then $x = 1$ is a solution. If $p \equiv 3 \pmod{4}$, then by the remark to Theorem 4.7, no solutions exist. Finally, if $p = 4k + 1$, then let $x = 1 \cdot 2 \cdots (2k)$. Then

$$\begin{aligned}x^2 &\equiv 1 \cdot 2 \cdots (2k) \cdot (2k) \cdots 2 \cdot 1 \\ &\equiv 1 \cdot 2 \cdots (2k) \cdot (-2k) \cdots (-2) \cdot (-1) \quad \text{(multiplying by } 2k \text{ } -1\text{s)} \\ &\equiv 1 \cdot 2 \cdots (2k) \cdot (p-2k) \cdots (p-2) \cdot (p-1) \\ &\equiv (p-1)! \equiv -1 \pmod{p}.\end{aligned}$$

Theorem 4.10. Let p be a prime such that $p \equiv 1 \pmod{4}$. Then there exist positive integers x and y such that $p = x^2 + y^2$.

Proof. By Theorem 4.9, there exists an integer a such that $a^2 \equiv -1 \pmod{p}$. Consider the set of integers of the form $ax - y$, where x and y are integers, $0 \leq x, y < \sqrt{p}$. The number of possible pairs (x, y) is then $(\lfloor \sqrt{p} \rfloor + 1)^2 > (\sqrt{p})^2 = p$, so by pigeonhole principle, there exist integers $0 \leq x_1, x_2, y_1, y_2 < \sqrt{p}$, such that $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$. Let $x = x_1 - x_2$ and $y = y_1 - y_2$. At least one of x and y is non-zero, and $ax \equiv y \Rightarrow a^2x^2 \equiv$

$-x^2 \equiv y^2 \Rightarrow x^2 + y^2 \equiv 0 \pmod{p}$. Thus, $x^2 + y^2$ is a multiple of p, and $0 < x^2 + y^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p$, so $x^2 + y^2 = p$.

Theorem 4.11. Let n be a positive integer. Then there exist integers x and y such that $n = x^2 + y^2$ iff each prime factor of n of the form $4k + 3$ appears an even number of times.

Theorem 4.12. *The Chinese Remainder Theorem (CRT).* If $a_1, a_2, \ldots, a_k$ are integers, and $m_1, m_2, \ldots, m_k$ are pairwise relatively prime integers, then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $m_1 m_2 \cdots m_k$.

Proof. Let $m = m_1 m_2 \cdots m_k$, and consider m/m_1. This is relatively prime to m_1, so there exists an integer t_1 such that $t_1 \cdot m/m_1 \equiv 1 \pmod{m_1}$. Accordingly, let $s_1 = t_1 \cdot m/m_1$. Then $s_1 \equiv 1 \pmod{m_1}$ and $s_1 \equiv 0 \pmod{m_j}$, $j \neq 1$. Similarly, for all i, there exists an s_i such that $s_i \equiv 1 \pmod{m_i}$ and $s_i \equiv 0 \pmod{m_j}$, $j \neq i$. Then, $x = a_1 s_1 + a_2 s_2 + \cdots + a_k s_k$ is a solution to the above system. To see uniqueness, let x' be another solution. Then $x - x' \equiv 0 \pmod{m_i}$ for all $i \Rightarrow x - x' \equiv 0 \pmod{m_1 m_2 \cdots m_k}$.

Remark. The proof shows explicitly how to find the solution x.

Example 4.9. For a positive integer n, find the number of solutions of the congruence $x^2 \equiv 1 \pmod{n}$.

Solution. Let the prime factorization of n be $2^e p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. By CRT, $x^2 \equiv 1 \pmod{n} \Leftrightarrow x^2 \equiv 1 \pmod{p_i^{e_i}}$ for all i, and $x^2 \equiv 1 \pmod{2^e}$. We consider these cases separately.

We have that $x^2 \equiv 1 \pmod{p_i^{e_i}} \Leftrightarrow x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p_i^{e_i}}$. But p_i cannot divide both $x - 1$ and $x + 1$, so it divides one of them; that is, $x \equiv \pm 1 \pmod{p_i^{e_i}}$. Hence, there are two solutions.

Now, if $(x - 1)(x + 1) \equiv 0 \pmod{2^e}$, 2 can divide both $x - 1$ and $x + 1$, but 4 cannot divide both. For $e = 1$ and $e = 2$, it is easily checked that there are 1 and 2 solutions respectively. For $e \geq 3$, since there is at most one factor

of 2 in one of $x-1$ and $x+1$, there must be at least $e-1$ in the other, for their product to be divisible by 2^e. Hence, the only possibilities are $x-1$ or $x+1 \equiv 0,\ 2^{e-1} \pmod{2^e}$, which lead to the four solutions $x \equiv 1,\ 2^{e-1}-1$, $2^{e-1}+1$, and 2^e-1.

Now that we know how many solutions each prime power factor contributes, the number of solutions modulo n is simply the product of these, by CRT. The following table gives the answer:

e	Number of solutions
$0, 1$	2^k
2	2^{k+1}
≥ 3	2^{k+2}

Theorem 4.11. Let m be a positive integer, let a and b be integers, and let $k = \gcd(a, m)$. Then the congruence $ax \equiv b \pmod{m}$ has k solutions or no solutions according as $k \mid b$ or $k \nmid b$.

Problems

1. Prove that for each positive integer n there exist n consecutive positive integers, none of which is an integral power of a prime.

   (1989 IMO)

2. For an odd positive integer $n > 1$, let S be the set of integers x, $1 \leq x \leq n$, such that both x and $x+1$ are relatively prime to n. Show that
$$\prod_{x \in S} x \equiv 1 \pmod{n}.$$

3. Find all positive integer solutions to $3^x + 4^y = 5^z$.

   (1991 IMO Short List)

4. Let n be a positive integer such that $n+1$ is divisible by 24. Prove that the sum of all the divisors of n is divisible by 24.

   (1969 Putnam Mathematical Competition)

5. (Wolstenholme's Theorem) Prove that if
$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is expressed as a fraction, where $p \geq 5$ is a prime, then p^2 divides the numerator.

6. Let a be the greatest positive root of the equation $x^3 - 3x^2 + 1 = 0$. Show that $\lfloor a^{1788} \rfloor$ and $\lfloor a^{1988} \rfloor$ are both divisible by 17.

   (1988 IMO Short List)

7. Let $\{a_1, a_2, \ldots, a_n\}$ and $\{b_1, b_2, \ldots, b_n\}$ be complete residue systems modulo n, such that $\{a_1 b_1, a_2 b_2, \ldots, a_n b_n\}$ is also a complete residue system modulo n. Show that $n = 1$ or 2.

8. Let m, n be positive integers. Show that $4mn - m - n$ can never be a square.

   (1984 IMO Proposal)

5 Binomial Coefficients

For non-negative integers n and k, $k \leq n$, the **binomial coefficient** $\binom{n}{k}$ is defined as

$$\frac{n!}{k!(n-k)!},$$

and has several important properties. By convention, $\binom{n}{k} = 0$ if $k > n$.

In the following results, for polynomials f and g with integer coefficients, we say that $f \equiv g \pmod{m}$ if m divides every coefficient in $f - g$.

Theorem 5.1. If p is a prime, then the number of factors of p in $n!$ is

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots.$$

It is also

$$\frac{n - s_n}{p - 1},$$

where s_n is the sum of the digits of n when expressed in base p.

Theorem 5.2. If p is a prime, then

$$\binom{p}{i} \equiv 0 \pmod{p}$$

for $1 \le i \le p-1$.

Corollary 5.3. $(1+x)^p \equiv 1 + x^p \pmod{p}$.

Lemma 5.4. For all real numbers x and y, $\lfloor x+y \rfloor \ge \lfloor x \rfloor + \lfloor y \rfloor$.

Proof. $x \ge \lfloor x \rfloor \Rightarrow x + y \ge \lfloor x \rfloor + \lfloor y \rfloor \in \mathbb{Z}$, so $\lfloor x+y \rfloor \ge \lfloor x \rfloor + \lfloor y \rfloor$.

Theorem 5.5. If p is a prime, then

$$\binom{p^k}{i} \equiv 0 \pmod{p}$$

for $1 \le i \le p^k - 1$.

Proof. By Lemma 5.4,

$$\sum_{j=1}^{k} \left(\left\lfloor \frac{i}{p^j} \right\rfloor + \left\lfloor \frac{p^k - i}{p^j} \right\rfloor \right) \le \sum_{j=1}^{k} \left\lfloor \frac{p^k}{p^j} \right\rfloor,$$

where the LHS and RHS are the number of factors of p in $i!(p^k - i)!$ and $p^k!$ respectively. But, $\left\lfloor \frac{i}{p^k} \right\rfloor = \left\lfloor \frac{p^k - i}{p^k} \right\rfloor = 0$ and $\left\lfloor \frac{p^k}{p^k} \right\rfloor = 1$, so the inequality is strict, and at least one factor of p divides $\binom{p^k}{i}$.

Corollary 5.6. $(1+x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}$.

Example 5.1. Let n be a positive integer. Show that the product of n consecutive positive integers is divisible by $n!$.

Solution. If the consecutive integers are m, $m+1$, $\ldots$, $m+n-1$, then

$$\frac{m(m+1)\cdots(m+n-1)}{n!} = \binom{m+n-1}{n}.$$

Example 5.2. Let n be a positive integer. Show that

$$(n+1)\,\mathrm{lcm}\left(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right) = \mathrm{lcm}(1, 2, \ldots, n+1).$$

(AMM E2686)

Solution. Let p be a prime $\le n+1$ and let α (respectively β) be the highest power of p in the LHS (respectively RHS) of the above equality. Choose r so that $p^r \le n+1 < p^{r+1}$. Then clearly $\beta = r$. We claim that

$$\text{if } p^r \le m < p^{r+1}, \text{ then } p^{r+1} \nmid \binom{m}{k} \text{ for } 0 \le k \le m. \qquad (*)$$

Indeed, the number of factors of p in $\binom{m}{k}$ is

$$\gamma = \sum_{s=1}^{r} \left(\left\lfloor \frac{m}{p^s} \right\rfloor - \left\lfloor \frac{k}{p^s} \right\rfloor - \left\lfloor \frac{m-k}{p^s} \right\rfloor \right).$$

Since each summand in this sum is 0 or 1, we have $\gamma \leq r$; that is, (*) holds. For $0 \leq k \leq n$, let

$$a_k = (n+1)\binom{n}{k} = (n-k+1)\binom{n+1}{k} = (k+1)\binom{n+1}{k+1}.$$

By $(*)$, p^{r+1} does not divide any of the integers $\binom{n}{k}$, $\binom{n+1}{k}$, or $\binom{n+1}{k+1}$. Thus, p^{r+1} can divide a_k only if p divides each of the integers $n+1$, $n-k+1$, and $k+1$. This implies that p divides $(n+1)-(n-k+1)-(k+1) = -1$, contradiction. Therefore, $p^{r+1} \nmid a_k$. On the other hand, for $k = p^r - 1$, we have that $k \leq n$ and $a_k = (k+1)\binom{n+1}{k+1}$ is divisible by p^r. Therefore, $\beta = r = \alpha$.

Theorem 5.7. *Lucas's Theorem.* Let m and n be non-negative integers, and p a prime. Let

$$\begin{aligned} m &= m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0, \quad \text{and} \\ n &= n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0 \end{aligned}$$

be the base p expansions of m and n respectively. Then

$$\binom{m}{n} \equiv \binom{m_k}{n_k}\binom{m_{k-1}}{n_{k-1}} \cdots \binom{m_1}{n_1}\binom{m_0}{n_0} \pmod{p}.$$

Proof. By Corollary 5.6,

$$\begin{aligned} (1+x)^m &\equiv (1+x)^{m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0} \\ &\equiv (1+x)^{p^k m_k} (1+x)^{p^{k-1} m_{k-1}} \cdots (1+x)^{p m_1} (1+x)^{m_0} \\ &\equiv (1+x^{p^k})^{m_k} (1+x^{p^{k-1}})^{m_{k-1}} \cdots (1+x^p)^{m_1} (1+x)^{m_0} \pmod{p}. \end{aligned}$$

By base p expansion, the coefficient of x^n on both sides is

$$\binom{m}{n} \equiv \binom{m_k}{n_k}\binom{m_{k-1}}{n_{k-1}} \cdots \binom{m_1}{n_1}\binom{m_0}{n_0} \pmod{p}.$$

Corollary 5.8. Let n be a positive integer. Let $A(n)$ denote the number of factors of 2 in $n!$, and let $B(n)$ denote the number of 1s in the binary expansion of n. Then the number of odd entries in the n^{th} row of Pascal's Triangle, or equivalently the number of odd coefficients in the expansion of $(1+x)^n$, is $2^{B(n)}$. Furthermore, $A(n) + B(n) = n$ for all n.

Useful Facts

- For a polynomial f with integer coefficients and prime p,

$$[f(x)]^{p^n} \equiv f(x^{p^n}) \pmod{p}.$$

Problems

1. Let a and b be non-negative integers, and p a prime. Show that

$$\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p}.$$

2. Let a_n be the last non-zero digit in the decimal representation of the number $n!$. Is the sequence $a_1, a_2, a_3, \ldots$ eventually periodic?

   (1991 IMO Short List)

3. Find all positive integers n such that $2^n \mid (3^n - 1)$.

4. Find the greatest integer k for which 1991^k divides

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

   (1991 IMO Short List)

5. For a positive integer n, let $a(n)$ and $b(n)$ denote the number of binomial coefficients in the n^{th} row of Pascal's Triangle that are congruent to 1 and 2 modulo 3 respectively. Prove that $a(n) - b(n)$ is always a power of 2.

6. Let n be a positive integer. Prove that if the number of factors of 2 in $n!$ is $n - 1$, then n is a power of 2.

7. For a positive integer n, let

$$C_n = \frac{1}{n+1}\binom{2n}{n},$$

and $S_n = C_1 + C_2 + \cdots + C_n$.

Prove that $S_n \equiv 1 \pmod 3$ if and only if there exists a 2 in the base 3 expansion of $n+1$.

6 Order of an Element

We know that if a is relatively prime to m, then there exists a positive integer n such that $a^n \equiv 1 \pmod m$. Let d be the smallest such n. Then we say that d is the **order** of a modulo m, denoted by $\text{ord}_m(a)$, or simply $\text{ord}(a)$ if the modulus m is understood.

Theorem 6.1. If a is relatively prime to m, then $a^n \equiv 1 \pmod m$ iff $\text{ord}(a) \mid n$. Furthermore, $a^{n_0} \equiv a^{n_1}$ iff $\text{ord}(a) \mid (n_0 - n_1)$.

Proof. Let $d = \text{ord}(a)$. It is clear that $d \mid n \Rightarrow a^n \equiv 1 \pmod m$. On the other hand, if $a^n \equiv 1 \pmod m$, then by the division algorithm, there exist integers q and r such that $n = qd + r$, $0 \le r < d$. Then $a^n \equiv a^{qd+r} \equiv (a^d)^q a^r \equiv a^r \equiv 1 \pmod m$. But $r < d$, so $r = 0 \Rightarrow d \mid n$. The second part of the theorem follows.

Remark. In particular, by Euler's Theorem, $\text{ord}(a) \mid \phi(m)$.

Example 6.1. Show that the order of 2 modulo 101 is 100.

Solution. Let $d = \text{ord}(2)$. Then $d \mid \phi(101)$, or $d \mid 100$. If $d < 100$, then d divides $100/2$ or $100/5$; that is, d is missing at least one prime factor. However,

$$2^{50} \equiv 1024^5 \equiv 14^5 \equiv 196 \cdot 196 \cdot 14 \equiv (-6) \cdot (-6) \cdot 14 \equiv -1 \pmod{101},$$

and

$$2^{20} \equiv 1024^2 \equiv 14^2 \equiv -6 \pmod{101},$$

so $d = 100$.

Example 6.2. Prove that if p is a prime, then every prime divisor of $2^p - 1$ is greater than p.

Solution. Let $q \mid (2^p - 1)$, where q is a prime. Then $2^p \equiv 1 \pmod{q}$, so $\text{ord}(2) \mid p$. But $\text{ord}(2) \neq 1$, so $\text{ord}(2) = p$. And by Fermat's Little Theorem, $\text{ord}(2) \mid (q-1) \Rightarrow p \leq q-1 \Rightarrow q > p$.

In fact, for $p > 2$, q must be of the form $2kp + 1$. From the above, $\text{ord}(2) \mid (q-1)$, or $p \mid (q-1) \Rightarrow q = mp + 1$. Since q must be odd, m must be even.

Example 6.3. Let p be a prime that is relatively prime to 10, and let n be an integer, $0 < n < p$. Let d be the order of 10 modulo p.

(a) Show that the length of the period of the decimal expansion of n/p is d.

(b) Prove that if d is even, then the period of the decimal expansion of n/p can be divided into two halves, whose sum is $10^{d/2} - 1$. For example, $1/7 = 0.\overline{142857}$, so $d = 6$, and $142 + 857 = 999 = 10^3 - 1$.

Solution. (a) Let m be the length of the period, and let $n/p = 0.\overline{a_1 a_2 \ldots a_m}$. Then

$$\frac{10^m n}{p} = a_1 a_2 \ldots a_m.\overline{a_1 a_2 \ldots a_m}$$

$$\Rightarrow \quad \frac{(10^m - 1)\, n}{p} = a_1 a_2 \ldots a_m,$$

an integer. Since n and p are relatively prime, p must divide $10^m - 1$, so d divides m. Conversely, p divides $10^d - 1$, so $(10^d - 1)n/p$ is an integer, with at most d digits. If we divide this integer by $10^d - 1$, then we obtain a rational number, whose decimal expansion has period at most d. Therefore, $m = d$.

(b) Let $d = 2k$, so $n/p = 0.\overline{a_1 a_2 \ldots a_k a_{k+1} \ldots a_{2k}}$. Now p divides $10^d - 1 = 10^{2k} - 1 = (10^k - 1)(10^k + 1)$. However, p cannot divide $10^k - 1$ (since the order of 10 is $2k$), so p divides $10^k + 1$. Hence,

$$\frac{10^k n}{p} = a_1 a_2 \ldots a_k.\overline{a_{k+1} \ldots a_{2k}}$$

$$\Rightarrow \quad \frac{(10^k + 1)\, n}{p} = a_1 a_2 \ldots a_k + 0.\overline{a_1 a_2 \ldots a_k} + 0.\overline{a_{k+1} \ldots a_{2k}}$$

is an integer. This can occur iff $a_1 a_2 \ldots a_k + a_{k+1} \ldots a_{2k}$ is a number consisting only of 9s, and hence, equal to $10^k - 1$.

Problems

1. Prove that for all positive integers $a > 1$ and n, $n \mid \phi(a^n - 1)$.

2. Prove that if p is a prime, then $p^p - 1$ has a prime factor that is congruent to 1 modulo p.

3. For any integer a, set $n_a = 101a - 100 \cdot 2^a$. Show that for $0 \leq a, b, c, d \leq 99$, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.

   (1994 Putnam Mathematical Competition)

4. Show that if $3 \leq d \leq 2^{n+1}$, then $d \nmid (a^{2^n} + 1)$ for all positive integers a.

7 Quadratic Residues

Let m be an integer greater than 1, and a an integer relatively prime to m. If $x^2 \equiv a \pmod{m}$ has a solution, then we say that a is a **quadratic residue** of m. Otherwise, we say that a is a **quadratic non-residue**. Now, let p be an odd prime. Then the **Legendre symbol**

$$\left(\frac{a}{p}\right)$$

is assigned the value of 1 if a is a quadratic residue of p. Otherwise, it is assigned the value of -1.

Theorem 7.1. Let p be an odd prime, and a and b be integers relatively prime to p. Then

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

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

Proof. If the congruence $x^2 \equiv a \pmod{p}$ has a solution, then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$, by Fermat's Little Theorem. If the congruence $x^2 \equiv a \pmod{p}$ has no solutions, then for each i, $1 \leq i \leq p-1$, there is a unique $j \neq i, 1 \leq j \leq p-1$, such that $ij \equiv a$. Therefore, all the integers from 1 to $p-1$ can be arranged into $(p-1)/2$ such pairs. Taking their product,

$$a^{(p-1)/2} \equiv 1 \cdot 2 \cdots (p-1) \equiv (p-1)! \equiv -1 \pmod{p},$$

by Wilson's Theorem. Part (b) now follows from part (a).

Remark. Part (a) is known as Euler's criterion.

Example 7.1. Show that if p is an odd prime, then

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0.$$

Solution. Note that 1^2, 2^2, ..., $((p-1)/2)^2$ are distinct modulo p, and that $((p+1)/2)^2$, ..., $(p-1)^2$ represent the same residues, simply in reverse. Hence, there are exactly $(p-1)/2$ quadratic residues, leaving $(p-1)/2$ quadratic non-residues. Therefore, the given sum contains $(p-1)/2$ 1s and $(p-1)/2$ -1s.

Theorem 7.2. *Gauss's Lemma.* Let p be an odd prime and let a be relatively prime to p. Consider the least non-negative residues of a, $2a$, ..., $((p-1)/2)a$ modulo p. If n is the number of these residues that are greater than $p/2$, then

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

Theorem 7.3. If p is an odd prime, then $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$; that is,

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

Proof. This follows from Theorem 4.9 (and Theorem 7.1).

Theorem 7.4. If p is an odd prime, then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$; that is,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

Proof. If $p \equiv 1$ or $5 \pmod 8$, then

$$\begin{aligned} 2^{(p-1)/2}\left(\frac{p-1}{2}\right)! &\equiv 2\cdot 4\cdot 6\cdots(p-1) \\ &\equiv 2\cdot 4\cdot 6\cdots\left(\frac{p-1}{2}\right)\cdot\left(-\frac{p-3}{2}\right)\cdots(-5)\cdot(-3)\cdot(-1) \\ &\equiv (-1)^{(p-1)/4}\left(\frac{p-1}{2}\right)! \\ \Rightarrow\ 2^{(p-1)/2} &\equiv (-1)^{(p-1)/4} \pmod p. \end{aligned}$$

By Theorem 7.1, $\left(\frac{2}{p}\right) = (-1)^{(p-1)/4}$. Hence, $\left(\frac{2}{p}\right) = 1$ or -1 according as $p \equiv 1$ or $5 \pmod 8$.

Similarly, if $p \equiv 3$ or $7 \pmod 8$, then

$$\begin{aligned} 2^{(p-1)/2}\left(\frac{p-1}{2}\right)! &\equiv 2\cdot 4\cdot 6\cdots\left(\frac{p-3}{2}\right)\cdot\left(-\frac{p-1}{2}\right)\cdots(-5)\cdot(-3)\cdot(-1) \\ &\equiv (-1)^{(p+1)/4}\left(\frac{p-1}{2}\right)! \\ \Rightarrow\ 2^{(p-1)/2} &\equiv (-1)^{(p+1)/4} \pmod p. \end{aligned}$$

Hence, $\left(\frac{2}{p}\right) = 1$ or -1 according as $p \equiv 7$ or $3 \pmod 8$.

Example 7.2. Prove that if n is an odd positive integer, then every prime divisor of $2^n - 1$ is of the form $8k \pm 1$. (Compare to Example 6.2)

Solution. Let $p \mid (2^n - 1)$, where p is prime. Let $n = 2m + 1$. Then $2^n \equiv 2^{2m+1} \equiv 2(2^m)^2 \equiv 1 \pmod p \Rightarrow \left(\frac{2}{p}\right) = 1 \Rightarrow p$ is of the form $8k \pm 1$.

Theorem 7.5. *The Law of Quadratic Reciprocity.* For distinct odd primes p and q,

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

Example 7.3. For which primes $p > 3$ does the congruence $x^2 \equiv -3 \pmod p$ have a solution?

Solution. We seek p for which $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1$. By quadratic reciprocity,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2} = \left(\frac{-1}{p}\right),$$

by Theorem 7.3. Thus, in general,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{-1}{p}\right)^2 = \left(\frac{p}{3}\right).$$

And, $(\frac{p}{3}) = 1$ iff $p \equiv 1 \pmod 3$. Since $p \not\equiv 4 \pmod 6$, we have that $x^2 \equiv -3 \pmod p$ has a solution iff $p \equiv 1 \pmod 6$.

Example 7.4. Show that if $p = 2^n + 1$, $n \geq 2$, is prime, then $3^{(p-1)/2} + 1$ is divisible by p.

Solution. We must have that n is even, say $2k$, for otherwise $p \equiv 0 \pmod 3$. By Theorem 7.1,

$$\left(\frac{3}{p}\right) \equiv 3^{(p-1)/2} \pmod p.$$

However, $p \equiv 1 \pmod 4$, and $p \equiv 4^k + 1 \equiv 2 \pmod 3 \Rightarrow \left(\frac{p}{3}\right) = -1$, and by quadratic reciprocity,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2} = 1,$$

so

$$\left(\frac{3}{p}\right) = -1 \;\Rightarrow\; 3^{(p-1)/2} + 1 \equiv 0 \pmod p.$$

Useful Facts

- (a) If p is a prime and $p \equiv 1$ or $3 \pmod 8$, then there exist positive integers x and y such that $p = x^2 + 2y^2$.
  (b) If p is a prime and $p \equiv 1 \pmod 6$, then there exist positive integers x and y such that $p = x^2 + 3y^2$.

Problems

1. Show that if $p > 3$ is a prime, then the sum of the quadratic residues among the integers 1, 2, ..., $p - 1$ is divisible by p.

2. Let F_n denote the n^{th} Fibonacci number. Prove that if $p > 5$ is a prime, then
$$F_p \equiv \left(\frac{p}{5}\right) \pmod p.$$

3. Show that 16 is a perfect 8^{th} power modulo p for any prime p.

4. Let a, b, and c be positive integers that are pairwise relatively prime, and that satisfy $a^2 - ab + b^2 = c^2$. Show that every prime factor of c is of the form $6k + 1$.

5. Let p be an odd prime and let ζ be a primitive p^{th} root of unity; that is, ζ is a complex number such that $\zeta^p = 1$ and $\zeta^k \neq 1$ for $1 \leq k \leq p-1$. Let A_p and B_p denote the set of quadratic residues and non-residues modulo p, respectively. Finally, let $\alpha = \sum_{k \in A_p} \zeta^k$ and $\beta = \sum_{k \in B_p} \zeta^k$. For example, for $p = 7$, $\alpha = \zeta + \zeta^2 + \zeta^4$ and $\beta = \zeta^3 + \zeta^5 + \zeta^6$. Show that α and β are the roots of

$$x^2 + x + \frac{1 - \left(\frac{-1}{p}\right) p}{4} = 0.$$

8 Primitive Roots

If the order of g modulo m is $\phi(m)$, then we say that g is a **primitive root** modulo m, or simply of m.

Example 8.1. Show that 2 is a primitive root modulo 3^n for all $n \geq 1$.

Solution. The statement is easily verified for $n = 1$, so assume the result is true for some $n = k$; that is, $2^{\phi(3^k)} \equiv 2^{2 \cdot 3^{k-1}} \equiv 1 \pmod{3^k}$. Now, let d be the order of 2 modulo 3^{k+1}. Then $2^d \equiv 1 \pmod{3^{k+1}} \Rightarrow 2^d \equiv 1 \pmod{3^k}$, so $2 \cdot 3^{k-1} \mid d$. However, $d \mid \phi(3^{k+1})$, or $d \mid 2 \cdot 3^k$. We deduce that d is either $2 \cdot 3^{k-1}$ or $2 \cdot 3^k$. Now we require the following lemma:

Lemma. $2^{2 \cdot 3^{n-1}} \equiv 1 + 3^n \pmod{3^{n+1}}$, for all $n \geq 1$.

This is true for $n = 1$, so assume it is true for some $n = k$. Then by assumption,

$$\begin{aligned} & 2^{2 \cdot 3^{k-1}} = 1 + 3^k + 3^{k+1} m \quad \text{for some integer } m \\ \Rightarrow \; & 2^{2 \cdot 3^k} = 1 + 3^{k+1} + 3^{k+2} M \quad \text{for some integer } M \text{ (obtained by cubing)} \\ \Rightarrow \; & 2^{2 \cdot 3^k} \equiv 1 + 3^{k+1} \pmod{3^{k+2}}. \end{aligned}$$

By induction, the lemma is proved.

Therefore, $2^{2 \cdot 3^{k-1}} \equiv 1 + 3^k \not\equiv 1 \pmod{3^{k+1}}$, so the order of 2 modulo 3^{k+1} is $2 \cdot 3^k$, and again by induction, the result follows.

Corollary 8.2. If $2^n \equiv -1 \pmod{3^k}$, then $3^{k-1} \mid n$.

Proof. The given implies $2^{2n} \equiv 1 \pmod{3^k} \Rightarrow \phi(3^k) \mid 2n$, or $3^{k-1} \mid n$.

Theorem 8.3. If m has a primitive root, then it has $\phi(\phi(m))$ (distinct) primitive roots modulo m.

Theorem 8.4. The positive integer m has a primitive root iff m is one of 2, 4, p^k, or $2p^k$, where p is an odd prime.

Theorem 8.5. If g is a primitive root of m, then $g^n \equiv 1 \pmod{m}$ iff $\phi(m) \mid n$. Furthermore, $g^{n_0} \equiv g^{n_1}$ iff $\phi(m) \mid (n_0 - n_1)$.

Proof. This follows directly from Theorem 6.1.

Theorem 8.6. If g is a primitive root of m, then the powers 1, g, g^2, $\ldots$, $g^{\phi(m)-1}$ represent each integer relatively prime to m uniquely modulo m. In particular, if $m > 2$, then $g^{\phi(m)/2} \equiv -1$ modulo m.

Proof. Clearly, each power g^i is relatively prime to m, and there are $\phi(m)$ integers relatively prime to m. Also, if $g^i \equiv g^j \pmod{m}$, then $g^{i-j} \equiv 1 \Rightarrow \phi(m) \mid (i-j)$ by Theorem 8.6, so each of the powers are distinct modulo m. Hence, each integer relatively prime to m is some power g^i modulo m. Furthermore, there is a unique i, $0 \leq i \leq \phi(m) - 1$, such that $g^i \equiv -1 \Rightarrow g^{2i} \equiv 1 \Rightarrow 2i = \phi(m)$, or $i = \phi(m)/2$.

Proposition 8.7. Let m be a positive integer. Then the only solutions to the congruence $x^2 \equiv 1 \pmod{m}$ are $x \equiv \pm 1 \pmod{m}$ iff m has a primitive root.

Proof. This follows from Example 4.9.

Example 8.2. For a positive integer m, let S be the set of positive integers less than m that are relatively prime to m, and let P be the product of the elements in S. Show that $P \equiv \pm 1 \pmod{m}$, with $P \equiv -1 \pmod{m}$ iff m has a primitive root.

Solution. We use a similar strategy as in the proof of Wilson's Theorem. The result is clear for $m = 2$, so assume that $m \geq 3$. We partition S as follows: Let A be the elements of S that are solutions to the congruence $x^2 \equiv 1 \pmod{m}$, and let B be the remaining elements. The elements in B can be arranged into pairs, by pairing each with its distinct multiplicative inverse. Hence, the product of the elements in B is 1 modulo m.

The elements in A may also be arranged into pairs, by pairing each with

its distinct additive inverse, i.e. x and $m - x$. These must be distinct, because otherwise, $x = m/2$, which is not relatively prime to m. Note that their product is $x(m - x) \equiv mx - x^2 \equiv -1 \pmod{m}$. Now if m has a primitive root, then by Proposition 8.7, A consists of only the two elements 1 and -1, so $P \equiv -1 \pmod{m}$. Otherwise, by Example 4.9, the number of elements of A is a power of two that is at least 4, so the number of such pairs in A is even, and $P \equiv 1 \pmod{m}$.

Remark. For m prime, this simply becomes Wilson's Theorem.

Theorem 8.8.

(1) If g is a primitive root of p, p a prime, then g or $g + p$ is a primitive root of p^2, according as $g^{p-1} \not\equiv 1 \pmod{p^2}$ or $g^{p-1} \equiv 1 \pmod{p^2}$.

(2) If g is a primitive root of p^k, where $k \geq 2$ and p is prime, then g is a primitive root of p^{k+1}.

By Theorem 8.6, given a primitive root g of m, for each a relatively prime to m, there exists a unique integer i modulo $\phi(m)$ such that $g^i \equiv a \pmod{m}$. This i is called the **index** of a with respect to the base g, denoted by $\operatorname{ind}_g(a)$ (i is dependent on g, so it must be specified). Indices have striking similarity to logarithms, as seen in the following properties:

(1) $\operatorname{ind}_g(1) \equiv 0 \pmod{\phi(m)}$, $\operatorname{ind}_g(g) \equiv 1 \pmod{\phi(m)}$,

(2) $a \equiv b \pmod{m} \Rightarrow \operatorname{ind}_g(a) \equiv \operatorname{ind}_g(b) \pmod{\phi(m)}$,

(3) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g(a) + \operatorname{ind}_g(b) \pmod{\phi(m)}$,

(4) $\operatorname{ind}_g(a^k) \equiv k \operatorname{ind}_g(a) \pmod{\phi(m)}$.

Theorem 8.9. If p is a prime and a is not divisible by p, then the congruence $x^n \equiv a \pmod{p}$ has $\gcd(n, p-1)$ solutions or no solutions according as

$$a^{(p-1)/\gcd(n,p-1)} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/\gcd(n,p-1)} \not\equiv 1 \pmod{p}.$$

Proof. Let g be a primitive root of p, and let i be the index of a with respect to g. Also, any solution x must be relatively prime to p, so let u be the index of x. Then the congruence $x^n \equiv a$ becomes $g^{nu} \equiv g^i \pmod{p} \Leftrightarrow nu \equiv i \pmod{p-1}$. Let $k = \gcd(n, p-1)$. Since g is a primitive root of p, $k \mid i \Leftrightarrow g^{i(p-1)/k} \equiv a^{(p-1)/k} \equiv 1$. The result now follows from Theorem 4.11.

Remark. Taking p to be an odd prime and $n = 2$, we deduce Euler's criterion.

Example 8.3 Let $n \geq 2$ be an integer and $p = 2^n + 1$. Show that if $3^{(p-1)/2} + 1 \equiv 0 \pmod{p}$, then p is a prime. (The converse to Example 7.4.)

Solution. From $3^{(p-1)/2} \equiv 3^{2^{n-1}} \equiv -1 \pmod{p}$, we obtain $3^{2^n} \equiv 1 \pmod{p}$, so the order of 3 is $2^n = p-1$, but the order also divides $\phi(p) \geq p-1$. Therefore, $\phi(p) = p - 1$, and p is a prime.

Example 8.4. Prove that if $n = 3^{k-1}$, then $2^n \equiv -1 \pmod{3^k}$. (A partial converse to Corollary 8.2.)

Solution. By Example 8.1, 2 is a primitive root of 3^k. Therefore, 2 has order $\phi(3^k) = 2 \cdot 3^{k-1} = 2n \Rightarrow 2^{2n} \equiv 1 \Rightarrow (2^n - 1)(2^n + 1) \equiv 0 \pmod{3^k}$. However, $2^n - 1 \equiv (-1)^{3^{k-1}} - 1 \equiv 1 \not\equiv 0 \pmod{3}$, so $2^n + 1 \equiv 0 \pmod{3^k}$.

Example 8.5. Find all positive integers $n > 1$ such that

$$\frac{2^n + 1}{n^2}$$

is an integer.

(1990 IMO)

Solution. Clearly, n must be odd. Now assume that $3^k \| n$; that is, 3^k is the highest power of 3 dividing n. Then $3^{2k} \mid n^2 \mid (2^n + 1) \Rightarrow 2^n \equiv -1 \pmod{3^{2k}} \Rightarrow 3^{2k-1} \mid n$, by Corollary 8.2 $\Rightarrow 2k - 1 \leq k \Rightarrow k \leq 1$, showing that n has at most one factor of 3. We observe that $n = 3$ is a solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $p \mid (2^n+1) \Rightarrow 2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d \mid 2n$. If d is odd, then $d \mid n \Rightarrow 2^n \equiv 1$, contradiction, so d is even, say $d = 2d_1$. Then $2d_1 \mid 2n \Rightarrow d_1 \mid n$. Also, $d \mid (p - 1)$, or $2d_1 \mid (p-1) \Rightarrow d_1 \leq (p-1)/2 < p$. But $d_1 \mid n$, so $d_1 = 1$ or $d_1 = 3$. If $d_1 = 1$, then $d = 2$, and $2^2 \equiv 1 \pmod{p}$, contradiction. If $d_1 = 3$, then $d = 6$, and $2^6 \equiv 1 \pmod{p}$, or $p \mid 63 \Rightarrow p = 7$. However, the order of 2 modulo 7 is 3, which is odd, again contradiction. Therefore, no such p can exist, and the only solution is $n = 3$.

Useful Facts

- All prime divisors of the Fermat number $2^{2^n} + 1$, $n > 1$, are of the form $2^{n+2}k + 1$.

Problems

1. Let p be an odd prime. Prove that

$$1^i + 2^i + \cdots + (p-1)^i \equiv 0 \pmod{p}$$

for all i, $0 \leq i \leq p-2$.

2. Show that if p is an odd prime, then the congruence $x^4 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{8}$.

3. Show that if a and n are positive integers with a odd, then $a^{2^n} \equiv 1 \pmod{2^{n+2}}$.

4. The number 142857 has the remarkable property that multiplying it by 1, 2, 3, 4, 5, and 6 cyclically permutes the digits. What are other numbers that have this property? Hint: Compute 142857×7.

9 Dirichlet Series

Despite the intimidating name, Dirichlet series are easy to work with, and can provide quick proofs to certain number-theoretic identities, such as Example 3.2. Let α be a function taking the positive integers to the integers. Then we say that

$$f(s) = \sum_{n=1}^{\infty} \frac{\alpha(n)}{n^s} = \alpha(1) + \frac{\alpha(2)}{2^s} + \frac{\alpha(3)}{3^s} + \cdots$$

is the **Dirichlet series generating function (Dsgf)** of the function α, which we denote by $f(s) \leftrightarrow \alpha(n)$. Like general generating functions, these generating functions are used to provide information about their corresponding number-theoretic functions, primarily through manipulation of the generating functions.

Let 1 denote the function which is 1 for all positive integers; that is, $1(n) = 1$ for all n. Let $\delta_1(n)$ be the function defined by

$$\delta_1(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

It is easy to check that 1 and δ_1 are multiplicative.

Now, let α and β be functions taking the positive integers to the integers. The **convolution** of α and β, denoted $\alpha * \beta$, is defined by

$$(\alpha * \beta)(n) = \sum_{d|n} \alpha(d)\beta(n/d).$$

Note that convolution is symmetric; that is, $\alpha * \beta = \beta * \alpha$.

Theorem 9.1. Let $f(s) \leftrightarrow \alpha(n)$ and $g(s) \leftrightarrow \beta(n)$. Then $(f \cdot g)(s) \leftrightarrow (\alpha * \beta)(n)$.

We now do three examples. The Dsgf of $1(n)$ is the well-known Riemann Zeta function $\zeta(s)$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots,$$

so $\zeta(s) \leftrightarrow 1(n)$. This function will play a prominent role in this theory. What makes this theory nice to work with is that we may work with these functions at a purely formal level; no knowledge of the analytic properties of $\zeta(s)$ or indeed of any other Dsgf is required.

By Theorem 9.1, the number-theoretic function corresponding to $\zeta^2(s)$ is

$$\sum_{d|n} 1(d)1(n/d) = \sum_{d|n} 1 = \tau(n).$$

Hence, $\zeta^2(s) \leftrightarrow \tau(n)$. Finally, it is clear that $1 \leftrightarrow \delta_1(n)$.

If α is a multiplicative function, then we can compute the Dsgf corresponding to α using the following theorem.

Theorem 9.2. Let α be a multiplicative function. Then

$$\sum_{n=1}^{\infty} \frac{\alpha(n)}{n^s} = \prod_p \sum_{k=0}^{\infty} \frac{\alpha(p^k)}{p^{ks}} = \prod_p [1 + \alpha(p)p^{-s} + \alpha(p^2)p^{-2s} + \alpha(p^3)p^{-3s} + \cdots],$$

where the product on the right is taken over all prime numbers.

As before, if we take $\alpha = 1$, then we obtain

$$\begin{aligned}\zeta(s) &= \prod_p (1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots) \\ &= \prod_p \left(\frac{1}{1 - p^{-s}}\right) \\ &= \frac{1}{\prod_p (1 - p^{-s})},\end{aligned}$$

an identity that will be useful.

We say that a positive integer $n > 1$ is **square-free** if n contains no repeated prime factors; that is, $p^2 \nmid n$ for all primes p. With this in mind, we define the Möbius function μ as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is not square-free, and} \\ (-1)^k & \text{if } n \text{ is square-free and has } k \text{ prime factors.} \end{cases}$$

It is easy to check that μ is multiplicative. By Theorem 9.2, the corresponding Dsgf is given by

$$\prod_p (1 - p^{-s}) = \frac{1}{\zeta(s)}.$$

Hence, $1/\zeta(s) \leftrightarrow \mu(n)$, and this property makes the the seemingly mysterious function μ very important, as seen in the following theorem.

Theorem 9.3. (Möbius Inversion Formula) Let α and β be functions such that

$$\beta(n) = \sum_{d|n} \alpha(d).$$

Then

$$\alpha(n) = \sum_{d|n} \mu(n/d)\beta(d).$$

Proof. Let $f(s) \leftrightarrow \alpha(n)$ and $g(s) \leftrightarrow \beta(n)$. The condition is equivalent to $\beta = \alpha * 1$, or $g(s) = f(s)\zeta(s)$, and the conclusion is equivalent to $\alpha = \beta * \mu$, or $f(s) = g(s)/\zeta(s)$.

Theorem 9.4. Let $f(s) \leftrightarrow \alpha(n)$. Then for any integer k, $f(s - k) \leftrightarrow n^k \alpha(n)$.

For more on Dirichlet series, and generating functions in general, see H. Wilf, *Generatingfunctionology.*

Problems

1. Let α, β, and γ be functions taking the positive integers to the integers.
   (a) Prove that $\alpha * \delta_1 = \alpha$.
   (b) Prove that $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$.
   (c) Prove that if α and β are multiplicative, then so is $\alpha * \beta$.

2. Prove that the following relations hold:
$$\begin{aligned} \frac{\zeta(s-1)}{\zeta(s)} &\leftrightarrow \phi(n), \\ \zeta(s)\zeta(s-1) &\leftrightarrow \sigma(n), \\ \frac{\zeta(s)}{\zeta(2s)} &\leftrightarrow |\mu(n)|. \end{aligned}$$

3. Let the prime factorization of a positive integer $n > 1$ be $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Define the functions λ and θ by $\lambda(n) = (-1)^{e_1+e_2+\cdots+e_k}$ and $\theta(n) = 2^k$. Set $\lambda(1) = \theta(1) = 1$. Show that λ and θ are multiplicative, and that
$$\frac{\zeta(2s)}{\zeta(s)} \leftrightarrow \lambda(n) \quad \text{and} \quad \frac{\zeta^2(s)}{\zeta(2s)} \leftrightarrow \theta(n).$$

4. For all positive integers n, let
$$f(n) = \sum_{m=1}^{n} \frac{n}{\gcd(m,n)}.$$
   (a) Show that $f(n) = \sum_{d|n} d\phi(d)$.
   (b) Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} > 1$ be the prime factorization of n. Show that
$$f(n) = \left(\frac{p_1^{2e_1+1}+1}{p_1+1}\right)\left(\frac{p_2^{2e_2+1}+1}{p_2+1}\right)\cdots\left(\frac{p_1^{2e_k+1}+1}{p_k+1}\right).$$

5. Verify Example 3.2 in one calculation.

6. Let id denote the identity function; that is, $\mathrm{id}(n) = n$ for all n. Verify each of the following identities in one calculation:

   (a) $\phi * \tau = \sigma$.

   (b) $\mu * 1 = \delta_1$.

   (c) $\mu * \mathrm{id} = \phi$.

   (d) $\phi * \sigma = \mathrm{id} \cdot \tau$.

   (e) $\sigma * \mathrm{id} = 1 * (\mathrm{id} \cdot \tau)$.

7. Let a_1, a_2, ..., be the sequence of positive integers satisfying

$$\sum_{d|n} a_d = 2^n$$

   for all n. Hence, $a_1 = 2$, $a_2 = 2^2 - 2 = 2$, $a_3 = 2^3 - 2 = 6$, $a_4 = 2^4 - 2 - 2 = 12$, and so on. Show that for all n, $n \mid a_n$.

   Hint: Don't use the Dsgf of $(a_n)_1^\infty$; use the Möbius Inversion Formula.

   Bigger Hint: Consider the function $f : [0, 1] \to [0, 1]$ defined by $f(x) = \{2x\}$, where $\{x\} = x - \lfloor x \rfloor$ is the fractional part of x. Find how the formula in the problem relates to the function $f^{(n)} = \underbrace{f \circ f \circ \cdots \circ f}_{n}$.

8. For all non-negative integers k, let σ_k be the function defined by

$$\sigma_k(n) = \sum_{d|n} d^k.$$

   Thus, $\sigma_0 = \tau$ and $\sigma_1 = \sigma$. Prove that

$$\zeta(s)\zeta(s-k) \leftrightarrow \sigma_k(n).$$

10 Miscellaneous Topics

10.1 Pell's Equations

Pell's equations (or Fermat's equations, as they are rightly called) are diophantine equations of the form $x^2 - dy^2 = N$, where d is a positive non-square integer. There always exist an infinite number of solutions when $N = 1$, which we characterize.

Theorem 10.1.1. If (a, b) is the lowest positive integer solution of $x^2 - dy^2 = 1$, then all positive integer solutions are of the form

$$(x_n, y_n) = \left(\frac{(a + b\sqrt{d})^n + (a - b\sqrt{d})^n}{2}, \ \frac{(a + b\sqrt{d})^n - (a - b\sqrt{d})^n}{2\sqrt{d}} \right).$$

We will not give a proof here, but we will verify that every pair indicated by the formula is a solution.

The pair (x_n, y_n) satisfy the equations

$$\begin{aligned} x_n + y_n\sqrt{d} &= (a + b\sqrt{d})^n, \text{ and} \\ x_n - y_n\sqrt{d} &= (a - b\sqrt{d})^n. \end{aligned}$$

Therefore,

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) \\ &= (a + b\sqrt{d})^n(a - b\sqrt{d})^n \\ &= (a^2 - db^2)^n \\ &= 1, \end{aligned}$$

since (a, b) is a solution.

Remark. The sequences (x_n), (y_n) satisfy the recurrence relations $x_n = 2ax_{n-1} - x_{n-2}$, $y_n = 2ay_{n-1} - y_{n-2}$.

For $x^2 - dy^2 = -1$, the situation is similar. If (a, b) is the least positive solution, then the (x_n, y_n) as above for n odd are the solutions of $x^2 - dy^2 = -1$, and the (x_n, y_n) for n even are the solutions of $x^2 - dy^2 = 1$.

Example 10.1.1 Find all solutions in pairs of positive integers (x, y) to the equation $x^2 - 2y^2 = 1$.

Solution. We find that the lowest positive integer solution is (3,2), so all positive integer solutions are given by

$$(x_n, y_n) = \left(\frac{(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n}{2}, \ \frac{(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n}{2\sqrt{2}} \right).$$

The first few solutions are (3,2), (17,12), and (99,70).

Example 10.1.2. Prove that the equation $x^2 - dy^2 = -1$ has no solution in integers if $d \equiv 3 \pmod 4$.

Solution. It is apparent that d must have a prime factor of the form $4k+3$, say q. Then $x^2 \equiv -1 \pmod q$, which by Theorem 4.9 is a contradiction.

Problems

1. In the sequence
$$\frac{1}{2}, \frac{5}{3}, \frac{11}{8}, \frac{27}{19}, \ldots,$$
the denominator of the n^{th} term $(n > 1)$ is the sum of the numerator and the denominator of the $(n-1)^{\text{th}}$ term. The numerator of the n^{th} term is the sum of the denominators of the n^{th} and $(n-1)^{\text{th}}$ term. Find the limit of this sequence.

   (1979 Atlantic Region Mathematics League)

2. Let $x_0 = 0$, $x_1 = 1$, $x_{n+1} = 4x_n - x_{n-1}$, and $y_0 = 1$, $y_1 = 2$, $y_{n+1} = 4y_n - y_{n-1}$. Show for all $n \geq 0$ that $y_n^2 = 3x_n^2 + 1$.

   (1988 Canadian Mathematical Olympiad)

3. The polynomials P, Q are such that deg $P = n$, deg $Q = m$, have the same leading coefficient, and $P^2(x) = (x^2 - 1)Q^2(x) + 1$. Show that $P'(x) = nQ(x)$.

   (1978 Swedish Mathematical Olympiad, Final Round)

10.2 Farey Sequences

The n^{th} **Farey sequence** is the sequence of all reduced rationals in [0,1], with both numerator and denominator no greater than n, in increasing order. Thus, the first 5 Farey sequences are:

0/1,										1/1,
0/1,					1/2,					1/1,
0/1,			1/3,		1/2,		2/3,			1/1,
0/1,		1/4,	1/3,		1/2,		2/3,	3/4,		1/1,
0/1,	1/5,	1/4,	1/3,	2/5,	1/2,	3/5,	2/3,	3/4,	4/5,	1/1.

Properties of Farey sequences include the following:

(1) If a/b and c/d are consecutive fractions in the same sequence, in that order, then $ad - bc = 1$.

(2) If a/b, c/d, and e/f are consecutive fractions in the same sequence, in that order, then

$$\frac{a+e}{b+f} = \frac{c}{d}.$$

(3) If a/b and c/d are consecutive fractions in the same sequence, then among all fractions between the two, $(a+c)/(b+d)$ (reduced) is the unique fraction with the smallest denominator.

For proofs of these and other interesting properties, see Ross Honsberger, "Farey Sequences", *Ingenuity in Mathematics*.

Problems

1. Let $a_1, a_2, \ldots, a_m$ be the denominators of the fractions in the n^{th} Farey sequence, in that order. Prove that

$$\frac{1}{a_1 a_2} + \frac{1}{a_2 a_3} + \cdots + \frac{1}{a_{m-1} a_m} = 1.$$

10.3 Continued Fractions

Let $a_0, a_1, \ldots, a_n$ be real numbers, all positive, except possibly a_0. Then let $\langle a_0, a_1, \ldots, a_n \rangle$ denote the **continued fraction**

$$a_0 + \cfrac{1}{a_1 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}.$$

If each a_i is an integer, then we say that the continued fraction is **simple**. Define sequences (p_k) and (q_k) as follows:

$$\begin{aligned} p_{-1} &= 0, \quad p_0 = a_0, \quad \text{and} \quad p_k = a_k p_{k-1} + p_{k-2}, \\ q_{-1} &= 0, \quad q_0 = 1, \quad \text{and} \quad q_k = a_k p_{k-1} + q_{k-2}, \quad \text{for } k \geq 1. \end{aligned}$$

Theorem 10.3.1. For all $x > 0$ and $k \geq 1$,

$$\langle a_0, a_1, \ldots, a_{k-1}, x \rangle = \frac{x p_{k-1} + p_{k-2}}{x q_{k-1} + q_{k-2}}.$$

In particular,

$$\langle a_0, a_1, \ldots, a_k \rangle = \frac{p_k}{q_k}.$$

Theorem 10.3.2. For all $k \geq 0$,

(1) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$,

(2) $p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k$.

Define c_k to be the k^{th} convergence $\langle a_0, a_1, \ldots, a_k \rangle = p_k/q_k$.

Theorem 10.3.3. $c_0 < c_2 < c_4 < \cdots < c_5 < c_3 < c_1$.

For a nice connection between continued fractions, linear diophantine equations, and Pell's equations, see Andy Liu, "Continued Fractions and Diophantine Equations", Volume 3, Issue 2, *Mathematical Mayhem*.

Problems

1. Let $a = \langle 1, 2, \ldots, 99 \rangle$ and $b = \langle 1, 2, \ldots, 99, 100 \rangle$. Prove that

$$|a - b| < \frac{1}{99!100!}.$$

(1990 Tournament of Towns)

2. Evaluate

$$\sqrt[8]{2207 - \cfrac{1}{2207 - \cfrac{1}{2207 - \cdots}}}.$$

Express your answer in the form $\frac{a+b\sqrt{c}}{d}$, where a, b, c, d are integers.

(1995 Putnam)

10.4 The Postage Stamp Problem

Let a and b be relatively prime positive integers greater than 1. Consider the set of integers of the form $ax + by$, where x and y are non-negative integers. The following are true:

(1) The greatest integer that cannot be written in the given form is $(a - 1)(b - 1) - 1 = ab - a - b$.

(2) There are $\frac{1}{2}(a-1)(b-1)$ positive integers that cannot be written in the given form.

(3) For all integers t, $0 \leq t \leq ab-a-b$, t can be written in the given form iff $ab-a-b-t$ cannot be.

(If you have not seen or attempted this enticing problem, it is strongly suggested you have a try before reading the full solution.)

Before presenting the solution, it will be instructive to look at an example. Take $a = 12$ and $b = 5$. The first few non-negative integers, in rows of 12, with integers that cannot be written in the given form in bold, are shown:

0	**1**	**2**	**3**	**4**	5	**6**	**7**	**8**	**9**	10	**11**
12	**13**	**14**	15	**16**	17	**18**	**19**	20	**21**	22	**23**
24	25	**26**	27	**28**	29	30	**31**	32	**33**	34	35
36	37	**38**	39	40	41	42	**43**	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59

With this arrangement, one observation should become immediately apparent, namely that bold numbers in each column end when they reach a multiple of 5. It should be clear that when reading down a column, once one hits an integer that can be written in the given form, then all successive integers can be as well, since we are adding 12 for each row we go down. It will turn out that this one observation is the key to the solution.

Proof. Define a **grapefruit** to be an integer that may be written in the given form. For each i, $0 \leq i \leq a-1$, let m_i be the least non-negative integer such that $b \mid (i + am_i)$. It is obvious that for $k \geq m_i$, $i + ak$ is a grapefruit. We claim that for $0 \leq k \leq m_i - 1$, $i + ak$ is not a grapefruit. It is sufficient to show that $i + a(m_i - 1)$ is not a grapefruit, if $m_i \geq 1$.

Let $i + am_i = bn_i$, $n_i \geq 0$. Since $i + a(m_i - b) = b(n_i - a)$, m_i must be strictly less than b; otherwise, we can find a smaller m_i. Then $i+a(m_i-b) \leq a-1-a = -1$, so $n_i < a$, or $n_i \leq a-1$. Suppose that $ax+by = i+a(m_i-1) = bn_i - a$, for some non-negative integers x and y. Then $a(x+1) = b(n_i - y)$, so $n_i - y$ is positive. Since a and b are relatively prime, a divides $n_i - y$. However, $n_i \leq a - 1 \Rightarrow n_i - y \leq a - 1$, contradiction.

Therefore, the greatest non-grapefruit is of the form $bn_i - a$, $n_i \leq a - 1$. The above argument also shows that all positive integers of this form are also non-grapefruits. Hence, the greatest non-grapefruit is $b(a-1)-a = ab-a-b$, proving (1).

Now, note that there are m_i non-grapefruits in column i. The above tells us the first grapefruit appearing in column i is $n_i b$. Since $0, b, 2b, \ldots, (a-1)b$ appear in different columns (because a and b are relatively prime), and there are a columns, we conclude that as i varies from 0 to $a-1$, n_i takes on 0, 1, $\ldots$, $a-1$, each exactly once. Therefore, summing over i, $0 \le i \le a-1$,

$$\begin{aligned}\sum_i (i + am_i) &= \sum_i i + \sum_i am_i = \frac{a(a-1)}{2} + a\sum_i m_i \\ &= \sum_i bn_i = \frac{a(a-1)b}{2} \\ \Rightarrow\ a\sum_i m_i &= \frac{a(a-1)(b-1)}{2} \\ \Rightarrow\ \sum_i m_i &= \frac{(a-1)(b-1)}{2},\end{aligned}$$

proving (2).

Finally, suppose that $ax_1 + by_1 = t$, and $ax_2 + by_2 = ab - a - b - t$, for some non-negative integers x_1, x_2, y_1, and y_2. Then $a(x_1 + x_2) + b(y_1 + y_2) = ab - a - b$, contradicting (1). So, if we consider the pairs $(t, ab - a - b - t)$, $0 \le t \le (a-1)(b-1)/2 - 1$, at most one element in each pair can be written in the given form.

However, we have shown that exactly $(a-1)(b-1)/2$ integers cannot be written in the given form, which is the number of pairs. Therefore, exactly one element of each pair can be written in the given form, proving (3).

Remark. There is a much shorter proof using Corollary 2.4. Can you find it?

For me, this type of problem epitomizes problem solving in number theory, and generally mathematics, in many ways. If I merely presented the proof by itself, it would look artificial and unmotivated. However, by looking at a specific example, and finding a pattern, we were able to use that pattern as a springboard and extend it into a full proof. The algebra in the proof is really nothing more than a translation of observed patterns into formal notation. (Mathematics could be described as simply the study of pattern.) Note also that we used nothing more than very elementary results, showing how powerful basic concepts can be. It may have been messy, but one should never be afraid to get one's hands dirty; indeed, the deeper you go, the

more you will understand the importance of these concepts and the subtle relationships between them. By trying to see an idea through to the end, one can sometimes feel the proof almost working out by itself. The moral of the story is: A simple idea can go a long way.

For more insights on the postage stamp problem, see Ross Honsberger, "A Putnam Paper Problem", *Mathematical Gems II*.

Problems

1. Let a, b, and c be positive integers, no two of which have a common divisor greater than 1. Show that $2abc - ab - bc - ca$ is the largest integer that cannot be expressed in the form $xab + yca + zab$, where x, y, and z are non-negative integers.

   (1983 IMO)

References

A. Adler & J. Coury, *The Theory of Numbers*, Jones and Bartlett

I. Niven & H. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons

Thanks to Ather Gattami for an improvement to the proof of the Postage Stamp Problem.