1998 IMO Camp

1 Divisibility

A non-zero integer a divides an integer b if there exists an integer c such that $b = ca$, which is denoted $a \mid b$; otherwise, a does not divide b, denoted $a \nmid b$. To indicate that $p^k \mid b$ but $p^{k+1} \nmid b$, i.e. p^k is the highest power of p dividing b, we may write $p^k \| b$, used only when p is a prime.

Useful Facts

$a, b > 0, a \mid b \Rightarrow a \leq b$

$a \mid b_1, a \mid b_2, \ldots, a \mid b_n \Rightarrow a \mid \sum_{i=1}^{n} b_i c_i, c_i \in Z$

Theorem 1.1. *The Division Algorithm.* Given integers a and b, $a > 0$, there exist unique integers q and r such that $b = qa + r$, $0 \leq r < a$, and $r = 0$ 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.

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

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

Example 1.2. Suppose that $a_1, a_2, \ldots, a_{2n}$ are distinct integers such that

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

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, and $(r - a_1) + (r - a_2) + \cdots + (r - a_{2n}) = 2nr - (a_1 + a_2 + \cdots + a_{2n}) = 1 + 2 + \cdots + n + (-1) + (-2) + \cdots + (-n) = 0 \Rightarrow r = (a_1 + a_2 + \cdots + a_{2n})/(2n)$.

Example 1.3. 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)

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

1. Given positive integers a and b such that $a \mid b^2$, $b^2 \mid a^3$, $a^3 \mid b^4$, $b^4 \mid a^5$, $\ldots$, 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 $(a+1/2)^n + (b+1/2)^n$ is an integer for only finitely many n.

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

5. Prove, for an arbitrary positive integer n, the inequality
$$0 < \sum_{k=1}^{n} \frac{g(k)}{k} - \frac{2n}{3} < \frac{2}{3},$$
   where $g(k)$ denotes the greatest odd divisor of k.

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

2 GCF and LCM

The greatest common factor of integers a and b is written $\gcf(a,b)$, and lowest common multiple, $\operatorname{lcm}(a,b)$. The integers a and b are relatively prime if $\gcf(a,b) = 1$.

Useful Facts
$\gcf(a,b)\ \operatorname{lcm}(a,b) = ab$
$\gcf(ma,mb) = m\ \gcf(a,b)$

If $d \mid a$, $d \mid b$, and $d > 0$, then $\gcf(a/d, b/d) = \gcf(a, b)/d$
(In particular, if $d = \gcf(a, b)$, then $\gcf(a/d, b/d) = 1$)
If $a \mid bc$, and $\gcf(b, c) = 1$, then $a \mid b$
If $a_1 a_2 \cdots a_n$ is a perfect kth power, and the a_i are pairwise relatively prime, then each a_i is a perfect kth power
Any two consecutive integers are relatively prime

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

Solution. Consider the $N+1$ numbers 1, 11, 111, ..., 111...1 ($N+1$ 1's). 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 numbers, a number 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 a number of the form 111...1, that remains divisible by N.

Theorem 2.1. Given integers a and b, there exist integers x and y such that $xa + yb = \gcf(a, b)$. Furthermore, as x and y range over all integers, $xa + yb$ takes on all multiples, and only multiples of $\gcf(a, b)$.

Proof. Let d be the smallest positive integer that $xa+yb$ attains. By the division algorithm, there exist integers q and r such that $a = qd + r$, $0 \leq r < d$. Then $r = a - qd = a - q(xa + yb) = (1 - qx)a - (qy)b$, so r is also a linear combination of a and b. But $r < d$, so $r = 0 \Rightarrow a = qd \Rightarrow d \mid a$, and similarly $d \mid b$. However, $\gcf(a, b) \mid (xa+yb)$ for all x and y, so $d = \gcf(a, b)$. The second part of the theorem follows.

Corollary 2.2. Integers a and b are relatively prime iff there exist x and y such that $xa + yb = 1$.

Example 2.2. Prove that the fraction $(21n + 4)/(14n + 3)$ is irreducible for every natural number n.

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

Example 2.3. Let $T_n = 2^{2^n} + 1$. Show that for $m, n \geq 0$, $m \neq n$, T_m is relatively prime to T_n.

Solution. We have

$$\begin{aligned} T_n - 2 = 2^{2^n} - 1 = 2^{2^{n-1} \cdot 2} - 1 = (T_{n-1} - 1)^2 - 1 = T_{n-1}^2 - 2T_{n-1} \\ = T_{n-1}(T_{n-1} - 2) = T_{n-1}T_{n-2}(T_{n-2} - 2) = \cdots \\ = T_{n-1}T_{n-2} \cdots T_1 T_0 (T_0 - 2) = T_{n-1}T_{n-2} \cdots T_1 T_0, \end{aligned}$$

for all $n \geq 1$. Therefore, any common factor 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. This result shows that there are an infinite number of primes.

The Euclidean Algorithm. By repeated use of the division algorithm, we may actually find the x and y in Theorem 2.1. For example, if we sought gcf(329,182),

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

and we stop when there is no remainder. The last dividend is the gcf, so in this case, gcf(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.

Useful Facts

Dirichilet's Theorem. If a and b are relatively prime, then the arithmetic sequence $\{an + b \mid n = 0, 1, \ldots\}$ contains infinitely many primes.

Example 2.4. 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 which 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 which are consecutive (and thus, relatively prime); otherwise, S cannot have greater than n elements. b) Consider the highest odd factor of each of the $n+1$ elements in S; each are among the n odd integers $1, 3, \ldots, 2n-1$. By the Pigeonhole principle, two must be same, and they differ (multiplication wise) by a power of 2, so one divides the other.

Example 2.5. Given positive integers $a_1, a_2, \ldots, a_n$, such that each is less than 1000, but $\text{lcm}(a_i, a_j) > 1000$ for all $i, j, i \neq j$. Show that $\sum_{i=1}^{n} \frac{1}{a_i} < 2$.

Solution. If $\frac{1000}{m} \geq a > \frac{1000}{m+1}$, then the m multiples $a, 2a, \ldots, ma$ do not exceed 1000. So, let k_1 the number of a_i in the interval $[1000, \frac{1000}{2})$, k_2 in $[\frac{1000}{2}, \frac{1000}{3})$, etc. Then there are $k_1 + 2k_2 + 3k_3 + \cdots$ numbers, no greater than 1000, which are multiples of at least

one of the a_i. But the multiples are distinct, so $k_1 + 2k_2 + 3k_3 + \cdots < 1000$. We have $2k_1 + 3k_2 + 4k_3 + \cdots = (k_1 + 2k_2 + 3k_3 + \cdots) + (k_1 + k_2 + k_3 + \cdots) < 1000 + n < 2000$. Therefore,

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

1. The symbols $(a, b, \ldots, g)$ and $[a, b, \ldots, g]$ denote the greatest common factor and lowest common multiples, 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 $\gcf(a^m - 1, a^n - 1) = a^{gcf(m,n)} - 1$, for positive integers a, m, and n.

3. 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)

4. The least common multiple of any two of the natural numbers $n \geq a_1 > a_2 > \cdots > a_k \geq 1$ does not exceed n. Prove that $ia_i \leq n$ for $i = 1, 2, \ldots, k$.

3 Numerical Functions

There are three important numerical functions. If the prime factorization of n 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

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

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

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

Also, $\phi(1)$, $\tau(1)$, and $\sigma(1)$ are defined to be 1.

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

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

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 $n = 1$, 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. Then each factor of n^2 determines a solution, and the converse is true, so the number of solutions is $\tau(n^2) = (2a_1 + 1)(2a_2 + 1) \cdots (2a_k + 1)$.

Example 3.2. Prove that $\sum_{d|n} \phi(d) = n$.

Solution. For a divisor d of n, let S_d be the set of all $1 \leq a \leq n$ such that $\gcf(a, n) = n/d$. Then, S_d consists of all elements of the form $b(n/d)$, where $0 \leq b \leq d$, and $\gcf(b, d) = 1$, so S_d contains $\phi(d)$ elements. Also, for all a, $1 \leq a \leq n$, a must belong to at least one S_d, but no two S_d can contain the same element. Therefore, each a belongs to a unique S_d. The result then follows from summing over all $d \mid n$.

1. Prove that

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

2. 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)

4 Modular Arithmetic

If $m \mid (a - b)$, we write $a \equiv b \pmod{m}$, otherwise, we write $a \not\equiv b \pmod{m}$ (although this notation is not used often). In the above notation, we are considering the integers modulo m.

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

$$(1)\ ak \equiv bk,\ (2)\ a + c \equiv b + d,\ (3)\ ac \equiv bd\ (mod\ m).$$

Useful Facts

If $a \equiv b \pmod{m}$, and f is a polynomial with integer coefficients, then $f(a) \equiv f(b) \pmod{m}$.

If f is a polynomial with integer coefficients of degree n, f not identically zero, and p is a prime, then $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

Example 4.1. Prove that the equation

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

has only the solution $x = y = z = 0$ in rational numbers.

Solution. Suppose the equation has a solution in rationals, with at least one non-zero value. 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. Now, taking the equation modulo 3, $x^3 \equiv 0 \pmod{3}$. Therefore, x must be divisible by 3, say $x_0 = 3x_1$. Substituting,

$$27x_1^3 + 3y_0^3 + 9z^3 - 27x_1y_0z_0 = 0 \Rightarrow 9x_1^3 + y_0^3 + 3z_0^3 - 9x_1y_0z_0 = 0.$$

Thus, 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 the solution (x_1, y_1, z_1). Thus, 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 pairs (F_k, F_{k+1}) modulo 10^4. Since there are a finite number of possible pairs (10^8 to be exact), and each pair is dependent only on the previous one, this sequence is ultimately periodic. Also, by the Fibonacci relation, one can find the previous term of 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 $10^4 \mid F_{7500}$, and (F_n) modulo 10^4 has period 15000, much smaller than the upper bound of 10^8.

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

Theorem 4.2. The inverse of a modulo m exists uniquely 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 then, a and m are relatively prime.

Now, if $\gcf(a, m) = 1$, then by Corollary 2.2, there exist x and y such that $xa + ym = 1 \Rightarrow ax = 1 - ym \Rightarrow ax \equiv 1 \pmod{m}$. Furthermore, the inverse x is unique, since

$ax \equiv ay \equiv 1 \Rightarrow ax - ay \equiv a(x-y) \equiv 0 \Rightarrow x - y \equiv 0$, or $x \equiv y \pmod{m}$.

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

Corollary 4.4. If $\gcf(k, m) = 1$, and $ak \equiv bk \pmod{m}$, then $a \equiv b \pmod{m}$

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

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

Proof. Let $a_1, a_2, \ldots, a_{\phi(m)}$ be the positive integers less than m that are relatively prime to m. Consider the integers $aa_1, aa_2, \ldots, aa_{\phi(m)}$. We claim that they are a permutation of the original $\phi(m)$ numbers 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 they are permuted. Hence, $a_1 a_2 \cdots a_{\phi(m)} \equiv (aa_1)(aa_2)\cdots(aa_{\phi(m)}) \Rightarrow a_1 a_2 \cdots a_{\phi(m)}(a^{\phi(m)} - 1) \equiv 0 \Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$.

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 4.3. Let S_i be the sum of the products of $1, 2, \ldots, p$, 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

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

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, so it must be the zero polynomial, and the result follows from comparing coefficients.

Remark. We also have $(p-1)! \equiv S_{p-1} \equiv -1 \pmod{p}$, 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 $p \mid (4x^2 + 1)$, then $p \equiv 1 \pmod{4}$.

Proof. Clearly, $p \neq 2$, so we need only show that $p \not\equiv 3 \pmod{4}$. Suppose $p = 4k + 3$ for some k. Let $y = 2x$, so by Fermat's Little Theorem, $y^{p-1} \equiv 1 \pmod{p}$, since x is relatively prime to p. But, $y^2 + 1 \equiv 0 \Rightarrow y^2 \equiv -1 \Rightarrow y^{p-1} \equiv y^{4k+2} \equiv y^{2(2k+1)} \equiv (-1)^{2k+1} \equiv -1$, contradiction. Therefore, $p \equiv 1 \pmod{4}$.

Example 4.4. Show that there are an infinite number of primes of the form $4k + 1$.

Solution. Suppose there are a finite number of primes of the form $4k + 1$. Let them be p_1, $p_2, \ldots, p_n$. Consider $N = 4(p_1 p_2 \cdots p_n)^2 + 1$. By Theorem 4.7, N must be divisible by a

prime of the form $4k+1$, but clearly, N is relatively prime to all such primes, contradiction.

Example 4.5. Show that if n is an integer, $n > 1$, then n does not divide $2^n - 1$.

Solution. Let p be the smallest prime divisor of n. Then $\gcf(n, p-1) = 1$, and there exist integers x and y such that $xn + y(p-1) = 1$. If $p \mid (2^n - 1)$, then $2 \equiv 2^{xn+y(p-1)} \equiv (2^n)^x (2^{p-1})^y \equiv 1 \pmod{p}$, contradiction. Therefore, $p(2^n - 1) \Rightarrow n(2^n - 1)$.

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

Proof. Consider the equation $x^2 \equiv 1 \pmod{p}$. Then $x^2 - 1 \equiv (x-1)(x+1) \equiv 0$, so the only solutions are $x \equiv 1$ and -1. Therefore, for each $2 \leq i \leq p-2$, there is a unique inverse $j \neq i$, $2 \leq j \leq p-2$, modulo p. Hence, when we group in pairs of inverses, $1 \cdot 2 \cdots (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdots 1 \cdot (p-1) \equiv -1 \pmod{p}$.

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

Proof. If $p = 2$, let $x = 1$. If $p \equiv 3 \pmod{4}$, then the proof of Theorem 4.7 shows that no solutions exist. Finally, if $p = 4k+1$, let $x = 1 \cdot 2 \cdots (2k)$. Then

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

Theorem 4.10. *The Chinese Remainder Theorem.* 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

$$\begin{aligned} x &\equiv a_1 \ (mod\, m_1), \\ x &\equiv a_2 \ (mod\, m_2), \\ &\cdots \\ x &\equiv a_k \ (mod\, m_k), \end{aligned}$$

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

First, consider the case when $a_1 = a_2 = \cdots = a_k = 0$. Then, $x \equiv 0 \pmod{m_i} \Rightarrow m_i \mid x \Rightarrow (m_1 m_2 \cdots m_k) \mid x$, or $x \equiv 0 \pmod{m_1 m_2 \cdots m_k}$, which is the unique solution we seek. Now, let $m = m_1 m_2 \cdots m_k$, and consider m/m_1. This is relatively prime to m_1, so there is a t_1 such that $t_1(m/m_1) \equiv 1 \pmod{m_1}$; accordingly, let $s_1 = t_1(m/m_1)$. Then $s_1 \equiv 1 \pmod{m_1}$ and $s_1 \equiv 0 \pmod{m_j}$, $j \neq 1$. Similarly, find 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

show uniqueness, if x_0 is another solution, then $x - x_0 \equiv 0 \pmod{m_i} \Rightarrow x - x_0 \equiv 0 \pmod{m_1 m_2 \cdots m_k}$, so by the above, the solution is unique modulo $m_1 m_2 \cdots m_k$.

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

Example 4.6. 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, $S \equiv b^{\phi(a)} \equiv 1 \pmod{a}$, and similarly $S \equiv a^{\phi(b)} \equiv 1 \pmod{b}$. Therefore, by the Chinese Remainder Theorem, $S \equiv 1 \pmod{ab}$.

Theorem 4.11. Let a, b, and $m > 0$ be integers, and let $k = \gcf(a, m)$. Then the congruence $ax \equiv b \pmod{m}$ has k solutions or no solutions according as $k \mid b$ or kb.

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 a positive integer $n > 2$, 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)

5. 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 $\lfloor x^{1788} \rfloor$ and $\lfloor x^{1988} \rfloor$ are both divisible by 17.

   (1988 IMO Short List)

5 Binomial Coefficients

The binomial coefficient $\binom{n}{k}$ is defined as $\dfrac{n!}{k!(n-k)!}$, and has several important properties.

Theorem 5.1. If p is a prime, then the highest power of p dividing $n!$ 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 $\dfrac{n - s_n}{p-1}$, 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 $1 \leq i \leq p-1$.

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

Lemma 5.4. $\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$ for all x, y.

Proof. $x \geq \lfloor x \rfloor \Rightarrow x + y \geq \lfloor x \rfloor + \lfloor y \rfloor \in Z$, so $\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$.

Theorem 5.5. If p is a prime, then $\binom{p^k}{i} \equiv 0 \pmod{p}$ for $1 \leq i \leq p^k - 1$.

Proof. We have $(i!(p^k - i)!) \mid (p^k)!$, since by Theorem 5.1 and Lemma 5.4,

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

but $\left\lfloor \dfrac{i}{p^k} \right\rfloor = \left\lfloor \dfrac{p^k - i}{p^k} \right\rfloor = 0$ and $\left\lfloor \dfrac{p^k}{p^k} \right\rfloor = 1$, so there is strict inequality, 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. Show that the product of n consecutive integers is divisible by $n!$.

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

$$x(x+1)\cdots(x+n-1)/n! = \binom{x+n-1}{n}.$$

Example 5.2. Show that

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

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

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

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 $\gamma \leq r$, i.e., $(*)$ 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 numbers $\binom{n}{k}$, $\binom{n+1}{k}$, or $\binom{n+1}{k+1}$. Thus, p^{r+1} can divide a_k only if p divides each of the numbers $n+1$, $n-k+1$, 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 $k \leq n$ and $a_k = (k+1)\binom{n+1}{k+1}$ is divisible by p^r. Therefore, $\beta = r = \alpha$.

Useful Facts
Given a polynomial f with integer coefficients, $[f(x)]^{p^n} \equiv f(x^{p^n}) \pmod{p}$, p prime.

1. 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)

2. If p is a prime and a, k are positive integers such that $p^k \mid (a-1)$, show that $p^{n+k} \mid (a^{p^n} - 1)$ for all positive integers n.

3. Find the highest k for which 1991^k divides the number $1990^{1991^{1992}} + 1992^{1991^{1990}}$.

   (1991 IMO Short List)

6 Order of an Element

If a is relatively prime to m, we know $a^n \equiv 1 \pmod{m}$ for some n. Let d be the smallest positive integer such that $a^d \equiv 1 \pmod{m}$. Then d is the order of a modulo m, denoted

ord(a).

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

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

Remark. In particular, ord(a) $\mid \phi(m)$.

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

Solution. Let $d = \text{ord}(2)$. By Fermat's Little Theorem, $2^{100} \equiv 1 \pmod{101}$, so $d \mid 100$. If $d < 100$, then d divides 100/2 or 100/5 (i.e. d is missing at least one prime factor). However,

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

and

$$2^{20} \equiv 1024^2 \equiv 14^2 \equiv -6 \ (mod\, 101),$$

so $d = 100$.

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

Solution. Assume $q \mid (2^p - 1)$, q prime. Then $2^p \equiv 1 \pmod{q}$, so ord(2) $\mid p$. But ord(2) $\neq 1$, so ord(2) $= p$. But by Fermat's Little Theorem, ord(2) $\mid (q-1) \Rightarrow p \leq q - 1 \Rightarrow q > p$. In fact, q must be of the form $2kp + 1$. From the above, ord(2) $\mid (q-1)$, or $p \mid (q-1) \Rightarrow q = mp + 1$. Since q must be odd, m is even.

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, which 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)

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

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 a is a quadratic residue of m; otherwise, it 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 -1.

Theorem 7.1. Let p be an odd prime, and a, b, be integers relatively prime to p. Then
(a) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,
(b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Proof. If $x^2 \equiv a$ has a solution, then $x^{p-1} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$.
If $x^2 \equiv a$ has no solutions, then for each $1 \leq i \leq p-1$, there is a unique $j \neq i, 1 \leq j \leq p-1$, such that $ij \equiv a$. Therefore, all numbers from 1 to $p-1$ can be arranged into $(p-1)/2$ such pairs. Taking the product, $1 \cdot 2 \cdots (p-1) \equiv (p-1)! \equiv a^{(p-1)/2} \equiv -1 \pmod{p}$, by Wilson's Theorem. Part (b) now follows from part (a).

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

Example 7.1. If p is an odd prime, show that

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

Solution. If a is relatively prime to p, then a is either a quadratic residue or non-residue modulo p. However, the residues satisfy $a^{(p-1)/2} \equiv 1$, so there can be no more than $(p-1)/2$ of them; similarly, there are no more than $(p-1)/2$ non-residues, so there must be exactly $(p-1)/2$ of both. Therefore, in the given sum, there are $(p-1)/2$ 1's and $(p-1)/2$ -1's. Another way to see that there are $(p-1)/2$ quadratic residues is to notice that $1^2, 2^2, \ldots,$ $((p-1)/2)^2$ are all distinct modulo p, and that $((p+1)/2)^2, \ldots, (p-1)^2$ represent the same residues.

Theorem 7.2. *Gauss' Lemma.* Let p be an odd prime and let a be relatively prime to p. Consider the least non-negative residues of $a, 2a, \ldots, ((p-1)/2)a$ 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 $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, i.e.

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

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

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

$\Rightarrow 2^{(p-1)/2} \equiv (-1)^{(p-1)/4} \pmod{p}$. So, 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

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

$\Rightarrow 2^{(p-1)/2} \equiv (-1)^{(p+1)/4} \pmod{p}$. 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 odd, then every prime divisor of $2^n - 1$ is of the form $8k \pm 1$. (Compare with Example 6.2)

Soltuion. Assume $p \mid (2^n - 1)$, p 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 7.4. *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 $x^2 \equiv -3 \pmod{p}$ 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, $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(1)(p-1)/2}$. But $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \pmod 3$, and -1 if $p \equiv 2 \pmod 3$.
Case 1 $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = 1$. Then $p \equiv 1 \pmod 4 \Rightarrow (-1)^{(p-1)/2} = 1 \Rightarrow \left(\frac{p}{3}\right) = 1 \Rightarrow p \equiv 1 \pmod 3 \Rightarrow p \equiv 1 \pmod{12}$.
Case 2 $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = -1$. Then $p \equiv 3 \pmod 4 \Rightarrow (-1)^{(p-1)/2} = -1 \Rightarrow \left(\frac{p}{3}\right) = 1 \Rightarrow p \equiv 1 \pmod 3 \Rightarrow p \equiv 7 \pmod{12}$.
Hence, $x^2 \equiv -3 \pmod p$ has a solution iff $p \equiv 1 \pmod 6$.

Example 7.4. Let p be a prime such that $p = 2^{2n} + 1$. Show that $3^{(p-1)/2} + 1$ is divisible by p.

Solution. By Theorem 1, $\left(\frac{3}{p}\right) \equiv 3^{(p-1)/2} \pmod p$. However, $p \equiv 1 \pmod 4$, and $p \equiv 4^n + 1 \equiv 2 \pmod 3 \Rightarrow \left(\frac{p}{3}\right) = -1$, and by Quadratic Reciprocity, $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(1)(p-1)/2} = 1$, so $\left(\frac{3}{p}\right) = -1 \Rightarrow 3^{(p-1)/2} + 1 \equiv 0 \pmod p$.

1. If $p > 3$ is a prime, then show that the sum of the quadratic residues among the numbers $1, 2, \ldots, p - 1$ is divisible by p.

2. Prove that if $p > 5$ is a prime, then $F_p \equiv \left(\frac{p}{5}\right) \pmod p$.

3. Show that the number 16 is a perfect 8th power (mod p) for any prime p.

8 Primitive Roots

If the order of g modulo m is $\phi(m)$, then 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 $n = k$, i.e. $2^{\phi(3^k)} \equiv 2^{2 \cdot 3^{k-1}} \equiv 1 \pmod{3^k}$. 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 $d \mid 2 \cdot 3^k$. From these two facts, $d = 2 \cdot 3^{k-1}$ or $2 \cdot 3^k$. Now we need the following

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, $2^{2 \cdot 3^{k-1}} = 1 + 3^k + 3^{k+1}m$ for some $m \Rightarrow 2^{2 \cdot 3^k} = 1 + 3^{k+1} + 3^{k+2}M$ for some integer $M \Rightarrow 2^{2 \cdot 3^k} \equiv 1 + 3^{k+1} \pmod{3^{k+2}}$. 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. 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 8.1. If m has a primitive root, then it has $\phi(\phi(m))$ (distinct) primitive roots.

Theorem 8.2. The 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 8.3. If g is a primitive root of m, then $g^n \equiv 1 \pmod{m} \Rightarrow \phi(m) \mid n$. Furthermore, $g^{n_0} \equiv g^{n_1} \Rightarrow \phi(m) \mid (n_0 - n_1)$.

Proof. This is a direct consequence of Theorem 6.1.

Theorem 8.4. 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, modulo m, uniquely.

Proof. Clearly, each 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 $g^{i-j} \equiv 1 \Rightarrow \phi(m) \mid (i - j)$, so each of the powers are distinct modulo m.

Example 8.2. Assume m has a primitive root, and S is the set of integers $1 \leq i \leq m$ that

are relatively prime to m. Find $\prod_{x \in S} x \pmod{m}$.

Solution. The result is easily verified for $m = 1$ and 2, so assume $m \geq 3$. Let g be a primitive root of m, and let $k = \phi(m)$. Then the elements of S are, possibly permuted, $1, g, g^2, \ldots, g^{k-1}$ modulo m. Thus, $\prod_{x \in S} x \equiv g^{1+2+\cdots+(k-1)} \equiv g^{k(k-1)/2} \pmod{m}$. Since $m \geq 3$, k is even and $k-1$ is odd. Since g is a primitive root of m, $g^{k/2} \equiv -1 \Rightarrow g^{k(k-1)/2} \equiv -1$, so $\prod_{x \in S} x \equiv -1 \pmod{m}$.

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

Theorem 8.5.
(1) If g is a primitive root of p, p 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 8.4, given a primitive root g of m, for each a relatively prime to m, there is a unique i modulo $\phi(m)$ such that $g^i \equiv a \pmod{m}$. This i is called the index of a with base g (i is dependent on the base, so it must be specified). Indices have striking similarity to logarithms, as seen in the following properties:
(1) ind $1 \equiv 0 \pmod{\phi(m)}$, ind $g \equiv 1 \pmod{\phi(m)}$,
(2) $a \equiv b \pmod{m} \Rightarrow$ ind $a \equiv$ ind $b \pmod{\phi(m)}$,
(3) ind $ab \equiv$ ind $a +$ ind $b \pmod{\phi(m)}$,
(4) ind $a^k \equiv k$ ind a $\pmod{\phi(m)}$, $k \geq 0$.

Theorem 8.6. If p is prime and a is relatively prime to p, then $x^n \equiv a \pmod{p}$ has $\gcf(n, p-1)$ solution or no solutions according as

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

Proof. Let g be a primitive root of p, and let i be the index of a with respect to g. If there is a solution x, then x and p are relatively prime, 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 $k = \gcf(n, p-1)$. The result follows from applying Theorem 4.11.

Remark. Taking p an odd prime and $n = 2$, we obtain Euler's Criterion.

Useful Facts
All prime divisors of the Fermat number $2^{2^n} + 1$ ($n > 1$) are of the form $2^{n+2}k + 1$.

Example 8.3. Prove that if $n = 3^{k-1}$, then $2^n \equiv -1 \pmod{3^k}$.

(A partial converse to the above corollary)

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 $2^n - 1$ is relatively prime to $3 \Rightarrow 2^n + 1 \equiv 0 \pmod{3^k}$.

Example 8.4. 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 $3^k \| n$, i.e. 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 the corollary $\Rightarrow 2k - 1 \leq k \Rightarrow k \leq 1$.
Suppose p is the smallest prime number > 3 dividing n, if it exists. 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 $d_1 \mid n$, contradiction, so such a p cannot exist, and the only possible solutions are 1 and 3. Therefore, the only solution is $n = 3$.

1. Prove that $1^i + 2^i + \cdots + (p - 1)^i \equiv 0 \pmod p$ for $0 \leq i \leq p - 2$, where p is an odd prime.

2. If p is an odd prime, show that $x^4 \equiv -1 \pmod p$ is solvable iff $p \equiv 1 \pmod 8$.

3. Show that if a is odd and $n \geq 1$, then $a^{2^n} \equiv 1 \pmod{2^{n+2}}$.

4. Let p be prime other than 2 or 5. Prove that 10 is a primitive root of p iff the decimal expansion of $1/p$ has period $p - 1$.

9 Miscellaneous Topics

9.1 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 non-negative non-square integer. There always exist

an infinite number of solutions when $N = 1$, and it is possible to characterize them.

Theorem 9.1.1. If (a, b) is the lowest positive solution of $x^2 - dy^2 = 1$, then all positive solutions are given by

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

Proof. First, we will show that every pair of the given form is a positive solution, with the following result:
Assume (a_1, b_1) and (a_2, b_2) are solutions of $x^2 - dy^2 = 1$. Define integers α, β by

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = \alpha + \beta\sqrt{d}.$$

Then, $\alpha = a_1a_2 + b_1b_2d$ and $\beta = a_1b_2 + a_2b_1$, so $(a_1 - b_1\sqrt{d})(a_2 - b_2\sqrt{d}) = \alpha - \beta\sqrt{d}$, and $\alpha^2 - d\beta^2 = (\alpha + \beta\sqrt{d})(\alpha - \beta\sqrt{d}) = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})(a_1 - b_1\sqrt{d})(a_2 - b_2\sqrt{d}) = (a_1^2 - db_1^2)(a_2^2 - db_2^2) = 1$. Therefore, (α, β) is another solution to $x^2 - dy^2 = 1$. A straightforward induction argument, using $(x_1, y_1) = (a, b)$ and this result shows that every (x_n, y_n) is indeed a solution. Furthermore, (x_1, y_1) is a positive solution, so all (x_n, y_n) are positive solutions. (A quick way of seeing that (x_n, y_n) is a solution is by observing that $x_n + y_n\sqrt{d} = (a + b\sqrt{d})^n$, and $x_n - y_n\sqrt{d} = (a - b\sqrt{d})^n \Rightarrow x_n^2 - dy_n^2 = (a + b\sqrt{d})^n(a - b\sqrt{d})^n = (a^2 - db^2)^n = 1$. We include the result above for use below.)
Now suppose (r, s) is a positive solution. Let $a' = r + s\sqrt{d}$, $a_n = x_n + y_n\sqrt{d}$, and $b_n = x_n - y_n\sqrt{d}$. Then $a_nb_n = 1 \Rightarrow b_n = 1/a_n > 0$. Also, $a_n < a_{n+1}$ since $a_n = a_1^n$ and $a_1 > 1$. Therefore, there exists an $n \geq 1$ such that $a_{n-1} < a' \leq a_n$. Multiplying by b_{n-1}, we obtain $1 < a'b_{n-1} \leq a_nb_{n-1} = a_1$.
Let $\gamma = a'b_{n-1}$, and define integers α and β by $\gamma = \alpha + \beta\sqrt{d}$. Then by the above, $\alpha^2 - d\beta^2 = 1$, since $(x_{n-1}, -y_{n-1})$ is also a solution of $x^2 - dy^2 = 1$. Let $\delta = \alpha - \beta\sqrt{d}$, so $\gamma\delta = \alpha^2 - d\beta^2 = 1$. Since $\gamma > 1, 0 < \delta < 1$. Therefore, α and β are positive. But $\gamma = \alpha + \beta\sqrt{d} \leq a_1 = a + b\sqrt{d}$. Since (a, b) is the least positive solution, $\alpha = a$ and $\beta = b$. Working backwards, $\gamma = a_1 \Rightarrow a' = a_n \Rightarrow r = x_n, s = y_n$.

For $x^2 - dy^2 = -1$, the situation is similar; the solutions are (x_n, y_n) for n odd, and the (x_n, y_n) for n even are the solutions of $x^2 - dy^2 = 1$.

Example 9.1.1. Prove that $x^2 - dy^2 = -1$ 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 $x^2 \equiv -1 \pmod q$, contradiction.

1. In the sequence

$$\frac{1}{2}, \frac{5}{3}, \frac{11}{8}, \frac{27}{19}, \cdots,$$

the denominator of the nth term ($n > 1$) is the sum of the numerator and the denominator of the $(n-1)$th term. The numerator of the nth term is the sum of the denominators of the nth and $(n-1)$th term. Find the limit of this sequence.

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 CMO)

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)

9.2 Farey Sequences

The nth 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:
(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 $(a+e)/(b+f) = c/d$.
(3) If a/b and c/d are consecutive fractions in the same sequence, then among all rational fractions with values between the two, $(a+c)/(b+d)$ is the unique fraction with the smallest denominator.
(4) If $0 \leq a \leq b$, with a and b relatively prime, then the fraction a/b first appears in the bth row.

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

9.3 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 the continued fraction is simple. Define sequences (p_k) and (q_k) as follows:

$$p_{-1} = 0,\ p_0 = a_0,\ \textit{and}\ p_k = a_k p_{k-1} + p_{k-2},$$
$$q_{-1} = 0,\ q_0 = 1,\ \textit{and}\ q_k = a_k p_{k-1} + q_{k-2},\ \textit{for}\ k \geq 1.$$

Theorem 9.3.1. For all $x > 0$ and $k \geq 1$, $\langle a_0, a_1, \ldots, a_{k-1}, x \rangle = (x p_{k-1} + p_{k-2})/(x q_{k-1} + q_{k-2})$. In particular, $\langle a_0, a_1, \ldots, a_k \rangle = p_k/q_k$.

Theorem 9.3.2. 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 kth convergence $\langle a_0, a_1, \ldots, a_k \rangle = p_k/q_k$.

Theorem 9.3.3. $c_0 < c_2 < c_4 < \cdots < c_5 < c_3 < c_1$.

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.*

1. Let $a = \langle 1, 2, \ldots, 99 \rangle$, and $b = \langle 1, 2, \ldots, 99, 100 \rangle$. Prove that $|a - b| < 1/(99!100!)$.
   (1990 Tournament of Towns)

9.4 The Postage Stamp Problem

Let a and b be relatively prime positive integers. Then consider the integers which may be written in the form $xa + yb$, where x and y are non-negative integers. Then:
(1) The greatest integer which cannot be written in the given form is $(a-1)(b-1) - 1 = ab - a - b$.
(2) For all integers $0 \leq t \leq ab - a - b$, t can be written in the given form iff $ab - a - b - t$ cannot be.

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

(This may not seem like the logical order of results, but it is the order we shall prove them. And if you have not seen or attempted this enticing problem, it is strongly suggested you have a try before seeing the full solution.)

Before presenting the solution, it will be instructive to look at an example. Take $a = 12$ and $b = 5$. Now, write the first few non-negative integers in rows of 12, with integers which cannot be written in the given form in bold, as 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: 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. Let a grapefruit be an integer which may be written in the given form. WOLOG, assume $a \geq b$. For an i such that $1 \leq i \leq a-1$, let m be the lowest non-negative integer such that $b \mid (i + ma)$. It is obvious that for $k \geq m$, $i + ka$ is a grapefruit. We claim that for $0 \leq k < m$, $i + ka$ is not a grapefruit. It is sufficient to show that $i + (m-1)a$ is not a grapefruit.
Assume $i + ma = nb$. Then $m < b$ and $n < a$, since $i + (m-b)a = b(n-a)$. Suppose $xa + yb = i + (m-1)a = nb - a$, for some integers x and y. Then $(x+1)a = b(n-y)$. Since a and b are relatively prime, a divides $n-y$, which is positive. However, $n < a \Rightarrow n - y < a$, contradiction.
Therefore, the greatest grapefruit must be of the form $nb-a$, $n < a$. The above argument also shows all positive integers of this form are also grapefruits. Hence, the greatest grapefruit is $(a-1)b - a = ab - a - b$.
Now we make a bold

Claim. Given i_1, i_2, such that $0 \leq i_1, i_2 \leq a-1$, and $i_1+i_2 \equiv -b \pmod{a}$. If $i_1+i_2 = a-b$, then for the corresponding m_i, $m_1+m_2 = b-1$. Otherwise, $i_1+i_2 = 2a-b$, and $m_1+m_2 = b-2$.

The sum $i_1 + i_2$ can only be $a-b$ or $2a-b$. Assume $i_1 + i_2 = a - b$. Now $b \mid (i_1 + m_1 a)$ and $b \mid (i_2+m_2 a) \Rightarrow i_1+i_2+(m_1+m_2)a \equiv a-b+(m_1+m_2)a \equiv (m_1+m_2+1)a \equiv 0 \Rightarrow m_1+m_2 \equiv -1 \pmod{b}$. Since $m_1, m_2 < b$, $m_1+m_2 \leq 2b-2 \Rightarrow m_1+m_2 = b-1$. Note that since $i_1+i_2 = a-b$, $i_1, i_2 \leq a-b$.

Now assume $i_1 + i_2 = 2a - b$. Since $i_1, i_2 < a$, $i_1, i_2 > a - b$. And again, $b \mid (i_1 + m_1 a)$ and $b \mid (i_2 + m_2 a) \Rightarrow i_1 + i_2 + (m_1 + m_2)a \equiv 2a - b + (m_1 + m_2)a \equiv (m_1 + m_2 + 2)a \equiv 0 \Rightarrow m_1 + m_2 \equiv -2 \pmod{b}$. Since $m_1, m_2 < b$, for $m_1 + m_2 = 2b - 2$ to hold, $m_1 = m_2 = b - 1$. However, $i_1 + m_1 a \equiv i_1 + (b-1)a \equiv i_1 - a \equiv 0 \pmod{b}$, so $i_1 \equiv a \pmod{b}$. Similarly, $i_2 \equiv a \pmod{b}$. But this is impossible, for $a - b < i_1, i_2 < a$. Therefore, $m_1 + m_2 = b - 2$.
Finally, we may prove (2). Given t, by the division algorithm, there exist unique integers k_1 and i_1 such that $t = k_1 a + i_1$, $0 \leq i_1 \leq a - 1$. Similarly, there exist unique integers k_2 and i_2 such that $ab - a - b - t = k_2 a + i_2$, $0 \leq i_2 \leq a - 1$. Then, $ab - a - b = (k_1 + k_2)a + i_1 + i_2$, so $i_1 + i_2 \equiv -b \pmod{a}$.
If $i_1 + i_2 = a - b$, then by the claim, $m_1 + m_2 = b - 1$. So, $ab - a - b = (k_1 + k_2)a + a - b \Rightarrow k_1 + k_2 = b - 2$. It is impossible that $k_1 \geq m_1$ and $k_2 \geq m_2$, or that $k_1 < m_1$ and $k_2 < m_2$, so exactly one of t and $ab - a - b - t$ is a grapefruit, establishing (2).
If $i_1 + i_2 = 2a - b$, then by the claim, $m_1 + m_2 = b - 2$. So, $ab - a - b = (k_1 + k_2)a + 2a - b \Rightarrow k_1 + k_2 = b - 3$. By the same argument as above, exactly one of t and $ab - a - b - t$ is a grapefruit.
Now, there are two easy ways of proving (3). First, it is a direct consequence of (1) and (2). Second, we may simply use the claim without the proof of (3). We may count the number of non-grapefruits, by counting them in pairs of columns, with $i_1 + i_2 = a - b$, and then $i_1 + i_2 = 2a - b$, obtaining the number

$$\frac{1}{2}(a - b + 1)(b - 1) + \frac{1}{2}(b - 1)(b - 2) = \frac{1}{2}(a - 1)(b - 1).$$

(With a bit of work, one can now prove (2) from (1) and (3). Can you see how?)

For me, this type of problem epitomizes the problem solving of 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 science 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.*

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 which cannot be expressed in the form $xab + yca + zab$, where x, y, and z are non-negative integers.

(1983 IMO)