Number Theory

Madhav R B

Contents

1 Divisibility **2**
1.1 Division Algorithm 2
1.2 Greatest Common Divisor (gcd) 2
1.3 Prime Numbers and Fundamental Theorem of Arithmetic 5

2 Congruence: **7**
2.1 Definitions and Basic Properties 7
2.2 Modular Inverse 7
2.3 Chinese Remainder Theorem 8
2.4 Euler's Totient Theorem & Fermat's Little Theorem 10
2.5 Modular Exponentiation 11
2.6 Wilson's Theorem 11

1 Divisibility

Definition: Let a and b be integers with $a \neq 0$. We say that a divides b, if there is an integer k such that $b = ak$. This is denoted by $a \mid b$.

- For every $a \neq 0$, $a \mid 0$ and $a \mid a$. Also, $1 \mid b$ for every b.
- If $a \mid b$ and $b \mid c$, then $a \mid c$.
- If $a \mid b$ and $a \mid c$, then $a \mid (sb + tc)$ for all integers s and t.

Prime Number: A number p > 1 whose positive divisors are only 1 and itself is called a prime number.

1.1 Division Algorithm

Theorem 1. *For every integer pair a, b, there exists distinct integer quotient and remainders, q and r, that satisfy*

$$a = b \cdot q + r, 0 \leq r < b$$

Proof: We have to prove that:

- For all integer pair (a, b) we can find a corresponding quotient and remainder
- This quotient and remainder pair are unique.

Let's prove this for positive integers a, b Consider the set:

$$\{a - bq \text{ with } q \in \mathbb{Z} \text{ and } a - bq \geq 0\}$$

This is a finite set with non-negative integers; hence, according to the well-ordering principle, it must have a minimum element, when $q = q_1$. $a - bq_1 = r \geq 0$. Assume r $r \geq b$, $a - bq_1 \geq b$ therefore $a - b(q_1 + 1) \geq 0$, hence $a - b(q_1 + 1)$ is also part of the set. However $a - b(q_1) > a - b(q_1 + 1)$, this contradicts the minimality of q_1. Hence $r < b$.
To prove uniqueness assume there exist q_1, q_2, r_1, r_2 such that $a = bq_1 + r_1 = bq_2 + r_2$ and $b(q_1 - q_2) = (r_2 - r_1)$, which implies $b|(r_1 - r_2)$. However $b > r_2 - r_1 > -b$ since $0 \leq r_1, r_2 < b$. Since $r_2 - r_1$ is a multiple of b, we must have $r_2 - r_1 = 0$ this implies $r_2 = r_1$ and $q_2 = q_1$.

Exercise 1. *Prove the case where any of a,b, or both a and b being negative.*

1.2 Greatest Common Divisor (gcd)

DefinitionThe greatest common divisor of a and b is the largest positive integer dividing both a and b and is denoted by either gcd(a, b) or by (a, b).
Note: Two numbers a and b are said to be co-prime if gcd(a,b)=1.

Theorem 1. *Euclid's Theorem: For natural numbers a and b, we use the division algorithm to determine a quotient and remainder, q and r, such that $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.*

Proof: Let d be a common divisor of $a\&b$. d must divide all linear combinations of a and b, and hence $d|a - bq = r$.Hence it's a common divisor of b and r. Let d' be a common divisor of b and r, it must divide all linear combinations of b and r, $r + bq = a$, thus it's a common divisor of a and b. Thus the set of common divisors of a and b, and b and r are equal. Hence the greatest among them must be equal.
Euclidean Algorithm: For two natural numbers a and b with $a > b$, to find $\gcd(a, b)$ we use the division algorithm repeatedly:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

Then we have $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{n-1},r_n) = r_n$.
This can be achieved by using the recursive function:

```
function GCD(a, b)
    if b = 0 then
        return a
    else
        return GCD(b, a mod b)
    end if
end function
```

Note: gcd(a,b,c) = gcd(gcd(a,b),c)

Theorem 2. *If $a(x) = b(x)q(x) + r(x)$ with $\deg(r(x)) < \deg(b(x))$, then*

$$\gcd(a(x), b(x)) = \gcd(b(x), r(x)).$$

For polynomials $a(x), b(x), q(x), r(x)$

Exercise 1. *What is the largest positive integer n such that $n^3 + 100$ is divisible by n+10?*

solution: Let

$$\begin{aligned} n^3 + 100 &= (n+10)(n^2 + an + b) + c \\ &= n^3 + n^2(10+a) + n(b+10a) + 10b + c \end{aligned}$$

Equating coefficients yields:

$$\begin{cases} 10 + a = 0 \\ b + 10a = 0 \\ 10b + c = 100 \end{cases}$$

Solving this system yields $a = -10$, $b = 100$, and $c = 900$. Therefore, by the Euclidean Algorithm, we get:

$$n + 10 = \gcd(n^3 + 100, n + 10) = \gcd(-900, n + 10) = \gcd(900, n + 10)$$

The maximum value for n is hence $n = 890$.

Exercise 2. *Let m,n be relatively prime positive integers. Calculate*

$$\gcd(5^m + 7^m, 5^n + 7^n)$$

.

solution: WLOG, let $m > n$. Note that

$$5^m + 7^m = (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^n 7^{m-n} - 5^{m-n} 7^n$$

We now have two cases.

- If $m < 2n$, then factor out $5^{m-n} - 7^{m-n}$ from the right hand side of the above equation in order to get
$$5^m + 7^m = (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^{m-n} 7^{m-n}(5^{2n-m} + 7^{2n-m})$$
Therefore, by the Euclidean Algorithm,
$$\gcd(5^m + 7^m, 5^n + 7^n) = \gcd(5^{m-n} 7^{m-n}(5^{2n-m} + 7^{2n-m}), 5^n + 7^n) = \gcd(5^{2n-m} + 7^{2n-m}, 5^n + 7^n)$$
Since 5 and 7 both do not divide $5^n + 7^n$.
- If $m > 2n$, then factor out $5^n 7^n$ from the right hand side of the first equation in order to get
$$5^m + 7^m = (5^n + 7^n)(5^{m-n} + 7^{m-n}) - 5^{m-n} 7^{m-n}(5^{m-2n} + 7^{m-2n})$$
Therefore, by the Euclidean Algorithm, and using the same logic as above,
$$\gcd(5^m + 7^m, 5^n + 7^n) = \gcd(5^n + 7^n, 5^{m-2n} + 7^{m-2n})$$

Let $a_{m,n} = \gcd(5^m + 7^m, 5^n + 7^n)$ for simplicity. In summary from the two cases above, if $m < 2n$, then $a_{m,n} = a_{n,2n-m}$. On the other hand, if $m > 2n$, then $a_{m,n} = a_{n,m-2n}$. If, for instance, we begin with $m = 12$ and $n = 5$, then the chain will go as follows:

$$a_{12,5} \to a_{2,5} \to a_{2,1} \to a_{0,1}$$

Note that each step in the process decreases the sum of the two values, and furthermore, the parity of the sum remains the same at each step. Since m and n are relatively prime and the process is invariant mod 2, if $m + n$ is odd, trying out a few other cases will reveal that following this chain always gives

$$a_{m,n} = a_{0,1} = \gcd(5^0 + 7^0, 5^1 + 7^1) = 2$$

On the other hand, if for instance $m = 13$ and $n = 5$, then the chain will go as follows:

$$a_{13,5} \to a_{5,3} \to a_{3,1} \to a_{1,1}$$

If $m + n$ is even, then we will always have

$$a_{m,n} = a_{1,1} = \gcd(5^1 + 7^1 - 5^1 + 7^1) = 12$$

In conclusion,

$$\gcd(5^m + 7^m, 5^n + 7^n) = \begin{cases} 12 & \text{if } 2 \mid (m+n) \\ 2 & \text{if } 2|(m+n) \end{cases}$$

Theorem 3. ***Bezout's Identity:*** *For natural numbers a and b, there exist x and y such that $ax+by = \gcd(a,b)$.*

Proof: Run the Euclidean Algorithm backwards.

$$\begin{aligned} \gcd(a,b) &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n \\ &= r_{n-2}(1 + q_n q_{n-1}) - r_{n-3}q_n \\ &\vdots \\ &= ax + by \\ &\in \mathbb{Z} \end{aligned}$$

Where x and y are some combination of the quotients. The two variables run through at every step in the equation are:

$$(r_{n-2}, r_{n-1}) \longrightarrow (r_{n-2}, r_{n-3}) \longrightarrow (r_{n-4} - r_{n-3}) \ldots (b, r_1) \longrightarrow (a, b)$$

This can be achieved using the algorithm that returns (x,y,gcd(a,b)) where ax+ by= gcd(a,b):

```
function PAIR_EGCD(a, b)
    if b = 0 then
        return 1, 0, a
    else
        x, y, gcd ← PAIR_EGCD(b, a mod b)
        return y, x − y × (a∇ · b), gcd
    end if
end function
```

Theorem 4. *If a— bc and gcd(ab) = 1 then a—c*

Proof: By Bézout's identity, $\gcd(a,b) = 1$ implies that there exist x and y such that $ax + by = 1$. Next, multiply this equation by c to arrive at

$$c(ax) + c(by) = c.$$

Finally, since $a \mid ac$ and $a \mid bc$, we have $a \mid c$.

Exercise 3. *Prove that the expression*

$$\frac{\gcd(m,n)\cdot\binom{n}{m}}{n}$$

is an integer for all pairs of integers $n \geq m \geq 1$

Solution: By Bezout's identity, there exist integers a and b such that $\gcd(m,n) = am + bn$. Next, notice that

$$\frac{\gcd(m,n)}{n} \cdot^n C_m = \frac{am+bn}{n} \cdot^n C_m = \frac{am}{n} \cdot^n C_m + b \cdot^n C_m$$

We mustnow prove that $\frac{am}{n} \cdot^n C_m$ is an integer. Note that:

$$\frac{m}{n} \cdot^n C_m = \frac{m}{n} \cdot \frac{n!}{m!(n-m)!} = \frac{(n-1)!}{(m-1)!(n-m)!} =^{n-1} C_{m-1}$$

Therefore,

$$\frac{\gcd(m,n)}{n} \cdot^m C_n = a \cdot^{m-1} C_{n-1} + b \cdot^m C_n$$

which is an integer

1.3 Prime Numbers and Fundamental Theorem of Arithmetic

Definition: Let n be a positive integer. Trivially, 1 and n divide n. If n ¿ 1 and no other positive integers besides 1 and n divide n, then we say n is prime. If n ¿ 1 but n is not prime, then we say that n is composite.

Theorem 1. ***Fundamental Theorem of Arithmetic*** *Every integer $n \geq 2$ has a unique prime factorization.*

Proof: Proving every integer greater than or equal to 2 has prime factorization using strong induction:

- Base case: n=2. Since 2 is a prime it can be written as 2^1
- Induction Hypothesis: Assume that for all i, $2 \leq i \leq k$, there exists a prime factorization for i.
- If k+1 is prime then it can be written as $(k+1)^1$, else there exist a prime $p < k+1$ that divides k+1. $k+1 = p \cdot \frac{k+1}{p}$, since $\frac{k+1}{p} < k+1$, there exist a prime factorization for it. Hence k+1 can be prime factorized whenever the induction hypothesis holds true.

Proving that this factorization is unique using induction:
The base case of $n = 2, 3, 4$ all have unique prime factorizations. Assume that every integer $n < k$ has a unique prime factorization, and we prove that $n = k$ must then have a unique prime factorization.

For the sake of contradiction, let k have two distinct prime factorizations, where repeated primes are allowed in the products:

$$k = p_1^{e_1} p_2^{e_2} \cdots p_i^{e_i} = q_1^{f_1} q_2^{f_2} \cdots q_j^{f_j}$$

Note that we must have $p_1 = q_m$ for some integer m with $1 \leq m \leq j$. By Euclid's Lemma (from Section 1.1), we know that p_1 must divide q_m. Therefore, $p_1 = q_m$ since they are primes. Now, we can cancel p_1 from both sides of the expression to get:

$$\frac{k}{p_1} = \frac{k}{q_m} = p_2^{e_2} \cdots p_i^{e_i} = q_1^{f_1} q_2^{f_2} \cdots q_{m-1}^{f_{m-1}} q_{m+1}^{f_{m+1}} \cdots q_j^{f_j}$$

By the inductive hypothesis, $\frac{k}{p_1} = \frac{k}{q_m}$ has a unique prime factorization. Therefore, the two products above contain the same exact primes with the same multiplicity (although they may be slightly rearranged). Similarly, since $p_1 = q_m$, the two initial products are exactly identical, and k has a unique prime factorization.

LCM(Least Common Multiple): For $a, b \in \mathbb{Z}$, a common multiple of a and b is an integer m such that a m and b m; moreover, such an m is the least common multiple of a and b if m is non-negative and m divides all common multiples of a and b.

Theorem 2. *Let the prime factorizations of two integers a and b be:*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
$$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

where the exponents e_i and f_i can be zero, and p_i are distinct primes.

Then,

$$\gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}$$

and

$$\text{lcm}[a,b] = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_k^{\max(e_k,f_k)}$$

Corollary 1.1. *For $a, b \in \mathbb{Z}^+$, $\gcd(a,b) \cdot \text{lcm}[a,b] = ab$.*

Exercise 1. *Given the polynomial $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ with integer coefficients $a_1, a_2, \ldots, a_n$, and given that there exist four distinct integers a, b, c, and d such that $f(a) = f(b) = f(c) = f(d) = 5$, show that there is no integer k such that $f(k) = 8$.*

Solution. Set $g(x) = f(x) - 5$. Since a, b, c, d are all roots of $g(x)$, we must have

$$g(x) = (x-a)(x-b)(x-c)(x-d)h(x)$$

for some $h(x) \in \mathbb{Z}[x]$. Let k be an integer such that $f(k) = 8$, giving $g(k) = f(k) - 5 = 3$. Using the factorization above, we find that

$$3 = (k-a)(k-b)(k-c)(k-d)h(x)$$

By the Fundamental Theorem of Arithmetic, we can only express 3 as the product of at most three distinct integers $(-3, 1, 1)$. Since $k-a, k-b, k-c, k-d$ are all distinct integers, we have too many terms in the product, leading to a contradiction.

Exercise 2. *Show that the cube roots of three distinct prime numbers cannot be three terms(not necessarily consecutive) of an arithmetic progression.*

Solution. Assume for the sake of contradiction that three such distinct primes exist, and let their cube roots be $\sqrt[3]{p_1}$, $\sqrt[3]{p_2}$, and $\sqrt[3]{p_3}$. By definition of an arithmetic sequence, set

$$\sqrt[3]{p_1} = a, \quad \sqrt[3]{p_2} = a + kd, \quad \sqrt[3]{p_3} = a + md \quad (m > k)$$

Subtracting gives:

$$\sqrt[3]{p_2} - \sqrt[3]{p_1} = kd$$
$$\sqrt[3]{p_3} - \sqrt[3]{p_1} = md$$

Multiply the first equation by m and the second by k in order to equate the two:

$$m(\sqrt[3]{p_2} - \sqrt[3]{p_1}) = k(\sqrt[3]{p_3} - \sqrt[3]{p_1}) \implies m \cdot \sqrt[3]{p_2} - m \cdot \sqrt[3]{p_1} = k \cdot \sqrt[3]{p_3} - k \cdot \sqrt[3]{p_1} = mkd$$

Rearranging this equation, we get:

$$m \cdot \sqrt[3]{p_2} - k \cdot \sqrt[3]{p_3} = (m-k) \cdot \sqrt[3]{p_1} \quad (1.1)$$

Now, cubing this gives and Using this equation and some rearrangement, we get:

$$m^3p_2 - 3(m^2p_2^{\frac{2}{3}})(kp_3^{\frac{1}{3}}) + 3(mp_2^{\frac{1}{3}})(k^2p_3^{\frac{2}{3}}) - k^3p_3 = (m-k)^3p_1$$

Moving the integer terms over to the RHS and factoring out $3(mp_2^{\frac{1}{3}})(kp_3^{\frac{1}{3}})$ from the LHS gives:

$$[3(mp_2^{\frac{1}{3}})(kp_3^{\frac{1}{3}})](kp_3^{\frac{1}{3}} - mp_2^{\frac{1}{3}}) = (m-k)^3p_1 - m^3p_2 + k^3p_3$$

From Equation (1.1), we know that $kp_3^{\frac{1}{3}} - mp_2^{\frac{1}{3}} = (k-m)p_1^{\frac{1}{3}}$ Therefore, substituting this into the above equation gives:

$$3(m\sqrt[3]{p_2})(k\sqrt[3]{p_3})((k-m)\sqrt[3]{p_1}) = (m-k)^3p_1 - m^3p_2 + k^3p_3$$

Leaving only the cube roots on the left-hand side gives:

$$\sqrt[3]{p_1p_2p_3} = \frac{(m-k)^3p_1 - m^3p_2 + k^3p_3}{3mk(k-m)} \quad (1.2)$$

2 Congruence:

2.1 Definitions and Basic Properties

Definition: Let a, b, n be integers with $n \neq 0$. We say that $a \equiv b \pmod{n}$ (read: a is congruent to b mod n) if $a - b$ is a multiple (positive, negative, or zero) of n.
If $a \equiv b \pmod{n}$ then $a = b + nk$ for some integer k.
Properties:

1. $a \equiv 0 \pmod{n}$ if and only if $n \mid a$.
2. $a \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$.
4. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Theorem 1. *Let a, b, c, d, n be integers with $n \neq 0$, and suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:*

$$a + c \equiv b + d \pmod{n}, \quad a - c \equiv b - d \pmod{n}, \quad ac \equiv bd \pmod{n}.$$

Proof:

$$a = b + nk \text{ and } c = d + n\ell, \text{ for integers } k \text{ and } \ell.$$

Then

$$a + c = b + d + n(k + \ell),$$

so

$$a + c \equiv b + d \pmod{n}.$$

The proof that $a - c \equiv b - d$ is similar.
For multiplication, we have

$$ac = bd + n(dk + b\ell + nk\ell),$$

so

$$ac \equiv bd \pmod{n}.$$

Theorem 2. *Let a, b, c, n be integers with $n \neq 0$ and with $\gcd(a, n) = 1$. If $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.*

Proof: Since $\gcd(a, n) = 1$, there exist integers x and y such that

$$ax + ny = 1.$$

Multiply by $b - c$ to obtain

$$(ab - ac)x + n(b - c)y = b - c.$$

Since $ab - ac$ is a multiple of n by assumption, and $n(b - c)y$ is also a multiple of n, we find that $b - c$ is a multiple of n.

This means that

$$b \equiv c \pmod{n}.$$

2.2 Modular Inverse

Definition: We say that the inverse of a number a modulo m when a and m are relatively prime is the number b such that $ab \equiv 1 \pmod{m}$. The inverse is denoted by a^{-1}

Theorem 1. *When $\gcd(a, m) = 1$, a always has a distinct inverse modulo m.*

Proof: Let a and m be relatively prime positive integers. Let the set of positive integers relatively prime to m and less than m be $R = \{a_1, a_2, \ldots, a_{\phi(m)}\}$. $S = \{aa_1 \pmod m, aa_2 \pmod m, \ldots, aa_{\phi(m)} \pmod m\}$. Every element of S is relatively prime to m. If we can prove that all elements of S are unique, we can prove that S and R are equal. For the sake of contradiction, assume

$$a \cdot a_x \equiv a \cdot a_y \pmod m$$

Since a and m are coprime:

$$(a_x \equiv a_y \mod m$$

hence x must be equal to y, therefore the elements of S are distinct $\pmod m$. Since $1 \in R$, there must be an element $a_x \in S$ such that $aa_x \equiv 1 \pmod m$.

Corollary 1.1. *The equation* $ax \equiv b \pmod m$ *always has a solution when* $\gcd(a, m) = 1$*.*

Proof: Take $x \equiv a^{-1}b(\pmod m)$

Exercise 1. *Let a and b be two relatively prime positive integers and consider the arithmetic progression $a, a+b, a+2b, a+3b, \ldots$. Prove that there are infinitely many pairwise relatively prime terms in the arithmetic progression.*

Solution. We use induction. The base case is trivial. Assume that we have a set with m elements that are all relatively prime. Let this set be $S = \{a + k_1b, a + k_2b, \ldots, a + k_mb\}$. Let the set $\{p_1, p_2, \ldots, p_n\}$ be the set of all distinct prime divisors of elements of S. I claim that we can construct a new element. Let

$$a + xb \equiv 1 \pmod{p_1p_2 \cdots p_n}$$

We know that there exists a solution in x to this equation which we let be $x = k_{m+1}$. Since $\gcd(a + k_{m+1}b, a + k_ib) = 1$, we have constructed a set with size $m + 1$ and we are done.

Finding Modular Inverse: gcd(a,n)=1 implies there exist integers (x,y) such that ax+ny=1. This implies $ax \equiv 1 \pmod n$, hence x is the modular inverse of a wrt n. Find (x,y) using the Extended Euclidean Algorithm.

2.3 Chinese Remainder Theorem

Theorem 1. ***Chinese Remainder Theorem:*** *The system of linear congruences*

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \\ \vdots \\ x \equiv a_n \pmod{b_n} \end{cases}$$

where $b_1, b_2, \ldots, b_n$ are pairwise relatively prime (i.e., $\gcd(b_i, b_j) = 1$ for $i \neq j$), has exactly one distinct solution for x modulo $b_1b_2 \cdots b_n$.

Proof: Let's prove this using induction

Base case ($n = 2$): Consider the system:

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$$

Let $S = \{kb_1 + a_1, 0 \leq k \leq b_2 - 1$. Since $ax \equiv b \pmod m$ always has a solution when gcd(a,n)=1, the equation $kb_1 + a_1 \equiv a_2 \pmod{b_2}$ has a distinct solution in k. Therefore, there is a unique solution modulo b_1b_2.

Inductive Hypothesis: Assume the system has a solution for $n = k$, i.e.,

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \\ \vdots \\ x \equiv a_k \pmod{b_k} \end{cases}$$

has a unique solution modulo $b_1 b_2 \cdots b_k$, let that be z. **Inductive Step:** Now, consider the system for $n = k+1$, it can be reduced to finding a solution for:

$$\begin{cases} x \equiv z \pmod{b_1 b_2 \cdots b_k} \\ x \equiv a_{k+1} \pmod{b_{k+1}} \end{cases}$$

This is equivalent to the base case where we proved CRT holds for n=2.
Finding the solution: Let x satisfy the system of congruences:

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_n \mod m_n \end{cases}$$

where all pairs $(m_1, m_2, \ldots, m_n)$ are coprime. Let x_m^{-1} denote the inverse of x modulo m, and let $X_k = \frac{m_1, m_2 \ldots m_n}{m_k}$.

Using this notation, a solution to the equations is:

$$x = a_1 X_1 X_{m_1}^{-1} + a_2 X_2 X_{m_2}^{-1} + \ldots a_n X_n X_{m_n}^{-1}$$

In this solution, for each $k = 1, 2, \ldots, n$:

$$a_k X_k X_{k_{m_k}}^{-1} \equiv a_k \mod m_k,$$

because $X_k X_{k_{m_k}}^{-1} \equiv 1 \mod m_k$.

Exercise 1. *Consider a number line consisting of all positive integers greater than 7. A hole punch traverses the number line, starting from 7 and working its way up. It checks each positive integer n and punches it if and only if $\binom{n}{7}$ is divisible by 12. As the hole punch checks more and more numbers, the fraction of checked numbers that are punched approaches a limiting number L. Find L.*

Solution: Note that

$$^{n}C_7 = \frac{n!}{(n-7)!7!} = \frac{n(n-1)(n-2)(n-3)(n-4)(n-5)(n-6)}{2^4 \cdot 3^2 \cdot 5 \cdot 7}$$

In order for this to be divisible by $12 = 2^2 \cdot 3$, the numerator must be divisible by $2^6 \cdot 3^3$. (We don't care about the 5 or the 7; by the Pigeonhole Principle these will be canceled out by factors in the numerator anyway.) Therefore we wish to find all values of n such that

$$2^6 \cdot 3^3 \mid n(n-1)(n-2)(n-3)(n-4)(n-5)(n-6)$$

We start by focusing on the factors of 3, as these are easiest to deal with. By the Pigeonhole Principle, the expression must be divisible by $3^2 = 9$. Now, if

$$n \equiv 0, 1, 2, 3, 4, 5, \text{ or } 6 \pmod 9$$

one of these seven integers will be a multiple of 9 as well as a multiple of 3, and so in this case the expression is divisible by 27. (Another possibility is if the numbers $n, n-3$, and $n-6$ are all divisible by 3, but it is easy to see that this case has already been accounted for.) Now, we have to determine when the product is divisible by 2^6. If n is even, then each of $n, n-2, n-4, n-6$ is divisible by 2, and in addition exactly two of those numbers must be divisible by 4. Therefore the divisibility is sure. Otherwise, n is odd, and $n-1, n-3$, and $n-5$ are divisible by 2.

- If $n-3$ is the only number divisible by 4, then in order for the product to be divisible by 2^6 it must also be divisible by 16. Therefore $n \equiv 3 \pmod{16}$ in this case.
- If $n-1$ and $n-5$ are both divisible by 4, then in order for the product to be divisible by 2^6 one of these numbers must also be divisible by 8. Therefore

$$n \equiv 1, 5 \pmod 8 \implies n \equiv 1, 5, 9, \text{ or } 13 \pmod{16}$$

Pooling all our information together, we see that ${}^nC_7$ is divisible by 12 if n is such that

$$n \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 9$$

$$n \equiv 0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 14 \pmod{16}$$

There are 7 possibilities modulo 9 and 13 possibilities modulo 16, so by CRT there exist $7 \cdot 13 = 91$ solutions modulo $9 \cdot 16 = 144$. Therefore, as more and more numbers n are checked, the probability that ${}^nC_7$ is divisible by 12 approaches $\frac{91}{144}$

2.4 Euler's Totient Theorem & Fermat's Little Theorem

Definition: Euler's ϕ function calculates the number of of integers $1 \le a \le n$ such that gcd(a,n)=1. Note: For two integers a,b such that gcd(a,b)=1, $\phi(ab) = \phi(a) \cdots \phi(b)$. This can be proved from the fact that product of two numbers where one is coprime to a and the other is coprime to b will be coprime to ab.

Theorem 1. *For any integer n, Euler's totient function $\phi(n)$ is defined as:*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is over the distinct primes p dividing n.

Corollary 1.1. *For a prime number p, $\phi(p) = p - 1$.*

Corollary 1.2. *For a prime number p, and a positive integer r, $\phi(p^r) = p^r \dot{(} 1 - \frac{1}{p})$*

Proof: Let's start by proving the corollaries.
For a prime p, all integers from 1 to p-1 are coprime to it.
For a prime power p^r, all integers from 1 to p^r except multiples of p are coprime to it. Number of multiple s of p less than or equal to p^r equals $\frac{p^r}{p} = p^{r-1}$. Hence $\phi(p^r) = p^r - p^{r-1} = p^r \cdots (1 - \frac{1}{p})$.
Now an integer n can be factorized into $p_1^{k_1} \cdots p_2^{k_2} \dots p_m^{k_m}$ according to the fundamental theorem of arithmetic. Since $p_i^{k_i}$ and $p_j^{k_j}$ are coprime, we can use $\phi(ab) = \phi(a)\phi(b)$ to compute $\phi(n)$.

Theorem 2. ***Euler's Totient Theorem*** *For a relatively prime to m, we have $a^{\phi(m)} \equiv 1 \pmod m$.*

proof: The sets $\{a_1, a_2, \dots, a_{\phi(m)}\}$ and $\{aa_1, aa_2, \dots, aa_{\phi(m)}\}$ are the same modulo m (see Theorem 1 in section 2.2). Therefore, the products of each set must be the same modulo m:

$$a^{(\phi(m))} \cdot a_1 \cdot a_2 \cdot \dots \cdot a_{\phi(m)} \equiv \cdot a_1 \cdot a_2 \cdot \dots \cdot a_{\phi(m)} \pmod m.$$

This simplifies to:

$$a^{(\phi(m))} \equiv 1 \pmod m.$$

Theorem 3. ***Fermat's Little Theorem:****For a relatively prime to a prime p, we have $a^p \equiv a \pmod p$.*

proof: Special case of Euler's Totient theorem, when m is prime. For a prime p, $\phi(p) = p - 1$.

Exercise 1. *Evaluate the sum:*

$$\left\lfloor \frac{2^0}{3} \right\rfloor + \left\lfloor \frac{2^1}{3} \right\rfloor + \left\lfloor \frac{2^2}{3} \right\rfloor + \dots + \left\lfloor \frac{2^{1000}}{3} \right\rfloor$$

Solution. Note that we have

$$2^x \equiv 1 \pmod 3 \text{ when } x \text{ is even}$$

$$2^x \equiv 2 \pmod 3 \text{ when } x \text{ is odd.}$$

Therefore,

$$\sum_{n=0}^{1000}\left\lfloor\frac{2^n}{3}\right\rfloor = 0+\sum_{n=1}^{500}\left(\left\lfloor\frac{2^{2n-1}}{3}\right\rfloor+\left\lfloor\frac{2^{2n}}{3}\right\rfloor\right)$$

$$=\sum_{n=1}^{500}\left(\frac{2^{2n-1}-2}{3}+\frac{2^{2n-1}-1}{3}\right)$$

$$=\frac{1}{3}\sum_{n=1}^{500}(2^{2n-1}+2^{2n}-1)=\frac{1}{3}\sum_{n=1}^{1000}2^n-500=\frac{1}{3}(2^{1001}-2)-500$$

2.5 Modular Exponentiation

To evaluate $a^n \pmod{m}$, for large values of n. We can use modular exponentiation. We calculate $a^{\frac{n}{2}} \mod m$, and use this to evaluate $a^n \pmod{m}$.

```
function POW(a, n, m)
    if n = 0 then
        return 1
    end if
    if n = 1 then
        return a mod m
    end if
    temp ← pow(a, floor(n/2), m) mod m
    if n mod 2 = 0 then
        return (temp × temp) mod m
    else
        return (temp × temp × (a mod m)) mod m
    end if
end function
```

Using Euler's Totient Theorem:

Since $a^{\phi(m)} \equiv 1 \pmod{m}$, we can calculate $a^{n \pmod{\phi(m)}} \pmod{m}$ to calculate $a^n \pmod{m}$.

2.6 Wilson's Theorem

Having seen the theory of congruences and modular arithmetic, let us now see an illutrious application in proving a seemingly non-trivial theorem:
Theorem: $(p-1)! \equiv -1 \mod p$ if and only if p is a prime
Proof: Case where p=2,3 can be checked manually. Let's prove for $p > 3$. Suppose that a is any one of the $p-1$ positive integers from 1 to p-1, and consider the linear congruence $ax \equiv 1 \mod p$. Then gcd(a,p)=1, hence this linear congruence will have a unique solution modulo p. Let that solution be $a^{'}$.
Since p is a prime $a = a^{'}$ iff a=1 or a=p-1. If we omit the numbers 1 and p-1, Let's group the remaining integers 2,3, $\cdots$ p-2 into pairs $a, a^{'}$ where $a \neq a^{'}$, such that their product $aa^{'} \equiv 1 \mod p$. When these (p-3)/2 congruence are multiplied together and the factors rearranged we get

$$(p-2)! \equiv 1 \mod p$$

Now multiply by p-1 on both sides.