1 Divisibility

Definition 1. We say an integer b is *divisible* by a nonzero integer a (denoted $a|b$ - read as "a divides b") if there is an integer n such that $b = an$. If no such n exists, we say b is not divisible by a (denoted $a \nmid b$ - read as "a does not divide b"). If $a|b$ we say a is a *factor* or *divisor* of b and b is a *multiple* of a. A positive divisor of b that is not b itself is called a *proper divisor* of b.

Properties of Divisibility

- If $a|b$ and $a|c$ then for any integers m and n, $a|(mb + nc)$.
- If $n \neq 0$, $an|bn$ if and only if $a|b$.
- If $a|b$ and $b|c$ then $a|c$.
- If $a|b$ and $b|a$ then $a = \pm b$.

The first property listed above is an incredibly useful tool in divisibility problems. We'll prove that it holds below.

Proposition 1. If $a|b$ and $a|c$ then for any integers m and n, $a|(mb + nc)$.

Proof. Since $a|b$, we know $b = ax$ for some integer x. Likewise, since $a|c$, we know $c = ay$ for some integer y. Then $mb + nc = m(ax) + n(ay) = a(mx + ny)$, so $a|(mb + nc)$ as desired.

□

Divisibility Rules

- n is divisible by 2 if its last digit is even.
- n is divisible by 3 if the sum of its digits is a multiple of 3.
- n is divisible by 4 if its last two digits form a number that is a multiple of 4.
- n is divisible by 5 if its last digit is a 0 or a 5.
- n is divisible by 6 if it is divisible by both 2 and 3 (use the above tests to check).
- n is divisible by 8 if its last three digits form a number that is a multiple of 8.
- n is divisible by 9 if the sum of its digits is a multiple of 9.
- n is divisible by 10 if its last digit is 0.
- n is divisible by 11 if the alternating sum of its digits is a multiple of 11.

Theorem 1 (Division Algorithm.)**.** Given any integers a and b, with $b \neq 0$, there exist unique integers q and r such that $a = qb + r, 0 \leq r < b$.

Proof. For the sake of saving space, we will assume that a and b are positive. This proof can be extended in a straightforward way to deal with other possible cases.

Consider the set of all integers of the form $a - bx$ such that x is an integer and $a - bx \geq 0$. Notice this set is non-empty; in particular a is in this set. By the well-ordering principle (which states that every non-empty set of positive integers contains a least element), we know there is some least element in this set (let's call this element r and the x used to produce it q). Thus $a = qb + r$.

We now need to prove that $0 \leq r < b$. Since we only allow non-negative values of $a - bx$ in our set, r must be greater than or equal to zero. Now suppose by way of contradiction that $b \leq r$. Then since $r < r + b$ (recall b is positive), we know $b \leq r < r + b$ or (subtracting b from each term) $0 \leq r - b < b$. Since $r - b = a - b(q + 1)$, this contradicts the minimality of r. Thus it must be the case that $r < b$ as required.

We have now established the existence of q and r such that $a = qb + r$ with $0 \leq r < b$. Next we will demonstrate the uniqueness of these values.

Suppose by way of contradiction that q and r are not unique. Then there exist non-equal pairs q_1, r_1 and q_2, r_2 that satisfy the given form. That is, $a = q_1 b + r_1 = q_2 b + r_2$. Without loss of generality, suppose $q_1 > q_2$. Subtracting, we see that $0 = b(q_1 - q_2) + (r_1 - r_2)$. Since $q_1 > q_2$, $q_1 - q_2 \geq 1$. This implies $r_2 - r_1 = b(q_1 - q_2) \geq b \cdot 1 = b$. But this implies that $r_2 \geq r_1 + b \geq b$ which contradicts q_2, r_2 being a valid pair satisfying the given form. Thus the assumption that the pairs were different must have been faulty, so q and r are unique.

□

Tips on Divisibility problems

- When in doubt, go back to the division algorithm! Often it is easier to see what is going on if you work with something in the form $b = an$ rather than $a|b$.
- The property "if $a|b$ and $a|c$ then for any integers m and n, $a|(mb + nc)$" will show up a lot. Get comfortable with applying it.
- Remember that what is true of one side of the equation must be true of the other side as well. If one side is divisible by 2, the other side must be as well. If one side is a perfect square, the other side must be as well.
- Looking at remainders can be helpful! For example, it turns out the only possible remainders a perfect square can have upon division by 4 are 0 and 1. Using this trick can help in a lot of different problems.
- Keep in mind that the division algorithm tells us that there are only so many remainders upon division by a particular number! In particular, if you divide by b, there are only b possible remainders.

2 Euclidean Algorithm, GCD and LCM

Definition 2 (Greatest Common Divisor.)**.** For integers a and b and positive integer d, if $d|a$ and $d|b$ we call d a *common divisor* of a and b. Unless $a = b = 0$, they have a *greatest common divisor* which we denote $\gcd(a, b)$. If $\gcd(a, b) = 1$ we say that a and b are *relatively prime*. The concept of relative primeness is separate from the notion of prime numbers and is central to much of number theory.

Definition 3 (Least Common Multiple.)**.** For nonzero integers a and b and positive integer m, if $a|m$ and $b|m$ we call m a *common multiple* of a and b. The *least common multiple* we denote by $\text{lcm}(a, b)$.

Euclidean Algorithm. The *Euclidean Algorithm* is a method for computing $\gcd(a, b)$ (suppose for simplicity that $a \geq b$... since $\gcd(a, b) = \gcd(b, a)$, we do not lose generality). Note that by the Division Algorithm, we know we can write

$$\begin{aligned}
a &= q_0 b + r_1 \quad && 0 < r_1 < b \\
b &= q_1 r_1 + r_2 \quad && 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 \quad && 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4 \quad && 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \quad && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + 0.
\end{aligned}$$

The process terminates because $r_1 < b$, so $r_1 \leq b - 1$. Then $r_2 < r_1$, so $r_2 \leq b - 2$, and so on. Since the numbers are decreasing and they are positive integers, at some point the process can't continue (i.e., you reach 0).

Theorem 2. The number r_n outputted by the Euclidean algorithm is the greatest common divisor of a and b.

Proof. Let $d = \gcd(a, b)$. Recall that if $d|a$ and $d|b$ then $d|(a - bq_1)$, so $d|r_1$. But then $d|b$ and $d|r_1$, so $d|b - r_1q_2 = r_2$. The process continues, so $d|r_n$. Now, from the equation $r_{n-1} = q_nr_n$ we see that $r_n|r_{n-1}$. Then $r_n|(r_n + q_{n-1}r_{n-1} = r_{n-2}$. But then $r_n|(r_{n-1} + q_{n-2}r_{n-2} = r_{n-3}$, and so on. Therefore $r_n|a$ and $r_n|b$. Therefore r_n is a common divisor of a, b, which implies that $r_n \leq d$. But since $d|r_n$ and $d > 0$, we have that $d \leq r_n$. This implies that $r_n = d$, which is what we wanted to prove.

□

Example
Find $\gcd(5403, 4731)$.

We use the Division Algorithm to write

$$\begin{aligned} 5403 &= 1 \cdot 4731 + 672 \\ 4731 &= 7 \cdot 672 + 27 \\ 672 &= 24 \cdot 27 + 24 \\ 27 &= 1 \cdot 24 + 3 \\ 24 &= 8 \cdot 3 + 0 \end{aligned}$$

Thus we have $\gcd(5403, 4731) = \gcd(4731, 672) = \cdots = \gcd(3, 0) = 3$.

Theorem 3 (Bezout's Theorem.)**.** For any integers a, b (not both zero), there exist integers x and y such that $\gcd(a, b) = ax + by$ (that is, the gcd of a and b can be written as a linear combination of a and b). In fact, $\gcd(a, b)$ is the smallest positive integer that can be expressed in this form.

Proof. Let $g = \gcd(a, b)$ and let ℓ be the smallest positive integer that can be written as a linear combination $ax + by$ for some integers x, y.

$\boxed{g \leq \ell}$ We know that since $g|a$ and $g|b$, $g|ax + by$. This implies $g|\ell$, so we know g must be less than or equal to ℓ.

$\boxed{g \geq \ell}$ We will show ℓ is a common divisor of a and b. Suppose by way of contradiction that ℓ does not divide both a and b. Say without loss of generality that $\ell \nmid a$. By Division Algorithm we know

$$a = q\ell + r \qquad 0 < r < \ell$$

But then notice

$$r = a - q\ell = a - (ax + by)q = a(1 - qx) + b(qy)$$

$1 - qx$ and qy are integers, so this is a linear combination of a and b. Since r must be positive but less than ℓ, this contradicts the minimality of ℓ. Thus our assumption must be flawed, and it must be the case that ℓ is a common divisor of a and b. Since g is by definition the greatest common div isor of a and b, $g \geq \ell$.

Since $g \geq \ell$ and $g \leq \ell$, we can conclude $g = \ell$. Thus, the greatest common divisor of a and b is the smallest positive integer that can be written as a linear combination of a and b.

□

Extended Euclidean Algorithm. While it's nice to know there exist x and y such that $\gcd(a, b) = ax+by$, it's not necessarily easily apparent what such x and y might be. Luckily, we have a method for finding values of x and y such that $\gcd(a, b) = ax + by$. We call this process the Extended Euclidean Algorithm. This process gives a different proof of Bezout's identity.

Example
Find x, y such that $5403x + 4731y = 3$.

For neatness, let $a = 5403, b = 4731$. There are two ways to do this process. We can go from the "top" down or we can start at the "bottom" and build up. Notice that the equations we are using are those we found via the Euclidean Algorithm to determine $\gcd(5403, 4731)$. We'll do the top down version first:

$$\begin{aligned}
5403 &= 1 \cdot a + 0 \cdot b \\
4731 &= 0 \cdot a + 1 \cdot b \\
672 &= 5403 - 4731 \\
&= 1 \cdot a - 1 \cdot b \\
27 &= 4731 - 7 \cdot 672 \\
&= b - 7(1 \cdot a - 1 \cdot b) \\
&= 8 \cdot b - 7 \cdot a \\
24 &= 672 - 24 \cdot 27 \\
&= (1 \cdot a - 1 \cdot b) - 24(8 \cdot b - 7 \cdot a) \\
&= 169 \cdot a - 193 \cdot b \\
3 &= 27 - 24 \\
&= (8 \cdot b - 7 \cdot a) - (169 \cdot a - 193 \cdot b) \\
&= 201 \cdot b - 176 \cdot a \\
&= 201 \cdot 4731 - 176 \cdot 5403
\end{aligned}$$

Or if you prefer to start from the bottom:

$$\begin{aligned}
3 &= 27 - 24 \\
&= 27 - (672 - 24 \cdot 27) \\
&= 25 \cdot 27 - 672 \\
&= 25(4731 - 7 \cdot 672) - 672 \\
&= 25 \cdot 4731 - 176 \cdot 672 \\
&= 25 \cdot 4731 - 176(5403 - 4731) \\
&= 201 \cdot 4731 - 176 \cdot 5403
\end{aligned}$$

Which method you use here is a matter of personal preference; use whichever makes the most sense to you. Notice that the results we get from the two methods are identical, namely $3 = 201 \cdot 4731 - 176 \cdot 5403$ so $x = -176$ and $y = 201$.

While this is one solution, it turns out there are actually infinitely many x, y pairs that satisfy $3 = 5403x + 4731y$. We'll see more about that later.

Some Useful Facts about GCD

- $\gcd(ca, cb) = c \cdot \gcd(a, b)$
- If $d|a$ and $d|b$ with $d > 0$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}\gcd(a, b)$.
- If $\gcd(a, c) = \gcd(b, c) = 1$ then $\gcd(ab, c) = 1$.
- If $\gcd(b, c) = 1$, then $gcd(a, b) \cdot gcd(a, c) = \gcd(a, bc)$.

3 Primes

Definition 4 (Prime Numbers.)**.** A positive integer $p > 1$ is *prime* if its only positive divisors are 1 and p. A positive integer $n > 1$ is *composite* if it is not prime. Note that 1 is neither prime nor composite.

One powerful technique in number theory is prime factorization, writing an integer as the product of powers of primes. It turns out that all positive integers greater than 1 have a *unique* prime factorization. We'll prove this below, but first we need a lemma.

Lemma 1. If p is prime and $p|ab$, then $p|a$ or $p|b$.

Proof. Suppose $p|ab$. If $p|a$, we're done. Suppose $p \not| a$. Then $(p, a) = 1$, so by Bezout's identity there exist integers m and n such that

$$am + pn = 1.$$

Now multiply by b and get $abm + pnb = b$. Since $p|ab$ and $p|p$, then $p|abm + pnb = b$. Which is what we wanted to prove.

□

Proposition 2. If p is prime and $p|a_1a_2a_3 \cdots a_n$, then p divides one of the a_i.

Proof. We proceed by induction on n.

Base Case: ($n = 2$) We use the Lemma we just proved. I.H.: Assume if p is prime and $p|a_1a_2a_3 \cdots a_n$, then p divides one of the a_i.

Inductive Step: Suppose p is prime and $p|a_1a_2a_3 \cdots a_na_{n+1}$. We let $a = a_1a_2 \cdots a_n$ and $b = a_{n+1}$. By our base case, we know $p|a$ or $p|b$. If $p|b$, then $p|a_{n+1}$ and our claim holds. Otherwise, $p|a$ or $p|a_1a_2a_3 \cdots a_n$ so by our induction hypothesis, p divides one of the a_i and our claim holds.

Thus, by the principle of mathematical induction, we have proven our claim.

□

Theorem 4 (Fundamental Theorem of Arithmetic.)**.** All positive integers $n > 1$ can be written uniquely (up to the ordering of primes) as a product of prime powers, $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$, $\alpha_i > 0, k > 0, p_i$ prime.

Proof. Let's prove the existence by using strong induction. We know $2, 3, 4, 5, 6$ can be factored into primes as $2, 3, 2^2, 5, 2 \cdot 3$, respectively. Those are our base cases. Now assume that all numbers j satisfying $2 \leq j \leq k$ for some $k \geq 6$ can be factored. If $k+1$ is prime, then $k+1$ is already factored. If $k+1$ is not prime, then it must be composite, so there exist a, b satisfying $k+1 = ab$ with $2 \leq a \leq b \leq k$. By the induction hypothesis, a and b can be factored into primes. But then the product of their factorizations is a factorization of $k+1$ into primes. Therefore, we've shown the existence of a factorization by strong induction.

Now we prove uniqueness. Suppose by way of contradiction that there exists an integer with two prime factorizations. Let M be the smallest such integer. Then

$$M = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_m^{\alpha_m} = q_1^{\beta_1}q_2^{\beta_2} \cdots q_n^{\beta_n}$$

where the p_i and q_i are primes, not all the same. By the previous proposition, since $p_1|M = q_1^{\beta_1}q_2^{\beta_2} \cdots q_n^{\beta_n}$, then $p_1|q_j$ for some j. However, since q_j and p_1 are prime, this implies $q_j = p_1$. Thus we can divide out:

$$p_1^{\alpha_1 - 1}p_2^{\alpha_2}p_3^{\alpha_3} \cdots p_m^{\alpha_m} = \frac{M}{p_1} = q_1^{\beta_1}q_2^{\beta_2} \cdots q_{j-1}^{\beta_{j-1}}q_j^{\beta_j - 1}q_{j+1}^{\beta_{j+1}} \cdots q_n^{\beta_n}.$$

Note that this means that $\frac{M}{p_1}$ has two different prime factorizations. Also since $p_1 > 1$, $\frac{M}{p_1}$ is less than M. But this contradicts M being smallest integer with two prime factorizations. Thus our assumption that such an M existed must have been flawed, and we know that all positive integers $n > 1$ can be written uniquely as a product of prime powers as desired.

□

Proposition 3. There are infinitely many primes.

Proof. Suppose by way of contradiction that there are finitely many primes. Then we can list them out: $p_1, p_2, \ldots, p_k$.

Consider the integer $n = p_1p_2 \cdots p_k + 1$. This is not divisible by any of the primes in our list (it leaves a remainder of 1 upon division by any of them), but by the fundamental theorem of arithmetic, n must have a prime factorization.

Then either n itself is prime and was missing from our list, or there is some smaller prime that divides n that was not in our list. This contradicts our assumption that we are able to list out all existing primes, so it must be the case that there are an infinite number of primes.

□

This proof can be made constructive in the following fashion. Let $q_1 = 2$. Now, let q_n be a prime divisor of $1 + q_1 q_2 \cdots q_{n-1}$. By the proof above, q_n is a new prime for each n, so you get an infinite sequence of primes. Let's play around with this sequence. $q_2|3$ so $q_2 = 3$, $q_3|2 \cdot 3 + 1 = 7$, so $q_3 = 7$. Similarly $q_4 = 43$. But then $q_5|2 \cdot 3 \cdot 7 \cdot 43 + 1 = 13 \cdot 139$. Therefore q_5 has two options, it can be 5 or it can be 139. To make the process deterministic, we can consider the following two sequences (called Euclid-Mullin sequences):

1. Let q_n be the least prime factor of $1 + q_1 q_2 \ldots q_{n-1}$. Then we have the first elements of the sequence are 2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739.

2. Let q_n be the greatest prime factor of $1 + q_1 q_2 \ldots q_{n-1}$. Then we have the first elements of the sequence are 2, 3, 7, 43, 139, 50207, 340999, 2365347734339, 4680225641471129.

The first sequence is conjectured to capture all the primes! It is an open question.

The second sequence has been proven (by Andrew Booker in 2012) to skip infinitely many primes. Below we show why it skips the prime 5.

Suppose $q_n = 5$ for some n. Since 5 is the greatest prime factor of $1 + q_1 q_2 \cdots q_{n-1}$, then

$$A = 1 + q_1 q_2 \cdots q_{n-1} = 2^a \cdot 3^b \cdot 5^c.$$

Since $q_1 = 2, q_2 = 3$, then A is not even and A is not a multiple of 3, therefore $A = 5^c$. The remainder of 5 when divided by 4 is 1, so the remainder of 5^c when divided by 4 is also 1. On the other hand, $q_1 = 2$ and q_i is odd for $i = 2, 3, \ldots, n-1$, so $q_1 q_2 \cdots q_{n-1}$ is even but not a multiple of 4. This implies $A \neq 4k + 1$ for any k. This contradicts that A has remainder 1 when divided by 4.

Primes and GCD

We already know one way to find the greatest common divisor of two numbers. Now let's look at an alternative method based on the prime factorizations of the numbers. As an example, let's consider $38808 = 2^3 \cdot 3^2 \cdot 7^2 \cdot 11$ and $36855 = 3^4 \cdot 5 \cdot 7 \cdot 13$.

First let's compute $\gcd(38808, 36855)$ using the Euclidean Algorithm:

$$\begin{aligned} 38808 &= 1 \cdot 36855 + 1953 \\ 36855 &= 18 \cdot 1953 + 1701 \\ 1953 &= 1 \cdot 1701 + 252 \\ 1701 &= 6 \cdot 252 + 189 \\ 252 &= 1 \cdot 189 + 63 \\ 189 &= 3 \cdot 63 + 0 \end{aligned}$$

Thus we have $\gcd(38808, 36855) = \gcd(36855, 1953) = \cdots = \gcd(189, 63) = 63$.

Notice that the prime factorization of 63 is $3^2 \cdot 7$. What relation does this have to the prime factorizations of the original numbers? It seems that the exponents on the primes are the minimum of the exponents in the original prime factorization.

Proposition 4. Given two integers a and b with prime factorizations $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}$ with $\alpha_i, \beta_i \geq 0$, then

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}.$$

Proof. Let $g = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$. Clearly $p_i^{\min(\alpha_i, \beta_i)}$ divides both $p_i^{\alpha_i}$ and $p_i^{\beta_i}$ so g divides a and b. Thus, g is a common divisor of a and b.

Notice any integer greater than g must have some prime p_j such that the exponent on p_j (say γ_j) is greater than $\min(\alpha_j, \beta_j)$. Suppose without loss of generality that for p_j, $\min(\alpha_j, \beta_j) = \alpha_j$. Then the given integer cannot divide a since $p_j^{\gamma_j}$ does not divide $p_j^{\alpha_j}$, and thus does not divide a. This concludes our proof.

□

Tips for Prime problems

- Prime factorization is a very common technique. Get comfortable with it!
- Parity arguments in particular (even vs. odd) are very useful! Keep them in mind; they'll pop up a lot (and not just in problems about primes).
- Though this sounds obvious, don't forget that a prime p's only divisors are 1 and itself. Often this comes in handy.
- Take advantage of numbers that appear in the problem. For example, if you're given 5 numbers and told to find all n such that all of them are prime, check what the remainder is for each number when divided by 5. (This will be a recurring pattern... you'll get this same advice for mods and bases.) This won't always help, but it's a good place to start.

4 Modular Arithmetic

Definition 5. We say that a is *congruent* to b *modulo* m (denoted $a \equiv b \pmod{m}$) if $m \mid (a-b)$ (this is often shortened to simply "b mod m"). We call m the *modulus*. Note that this is the same as saying that a and b leave the same remainder upon division by m.

Most of the time when we use mods to deal with a value a, we'll look at what number a is congruent to mod m between 0 and $m-1$ (i.e. the remainder of a upon division by m). We call this value the *residue* of a mod m. We will also often look at the value a is congruent to mod m between $-m+1$ and 0.

Properties of Mods:

- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$
- If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$ then $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$.
- If $a \equiv b \pmod{m}$ then $ca \equiv cb \pmod{m}$.
- If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$ then $a_1 b_1 \equiv a_2 b_2 \pmod{m}$.
- If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$.
- If $ca \equiv cb \pmod{m}$ then $a \equiv b \left(\mod \dfrac{m}{\gcd(m,c)}\right)$

Theorem 5 (Cancellation Theorem)**.** If $ax \equiv ay \pmod{m}$ and $\gcd(a,m) = 1$, then $x \equiv y \pmod{m}$.

Proof. Suppose $ax \equiv ay \pmod{m}$. This means $m|ax - ay$ or $m|a(x-y)$. Since $\gcd(m,a) = 1$, we know it must be the case that $m|(x-y)$ and thus $x \equiv y \pmod{m}$.

□

Using Modular Arithmetic we can figure out what day of the week it will be in 10 days, 100 days, 1 million days and even 10^{10^6} days. Today is Monday. In 10 days, it will be Thursday because $10 \equiv 3 \bmod 7$ and Monday plus 3 days is Thursday. Since $100 \equiv 2 \bmod 7$, then it will be Wednesday in 100 days. Since $10^6 \equiv 1 \bmod 7$, then it will be Tuesday in 1 million days. To calculate 10^{10^6} we need a bit more work. The first idea is that $10^6 \equiv 1 \bmod 7$. Since $10^6 \equiv 4 \bmod 6$, then $10^6 = 6k + 4$ for some integer k. But then

$$10^{10^6} = 10^{6k+4} = \left(10^6\right)^k \cdot 10^4 \equiv 1^k \cdot 10^4 \equiv 10^4 \equiv 4 \bmod 7.$$

Therefore it will be Friday in 10^{10^6} days (in the very hypothetical situation that the Sun hasn't exploded by then).

We can also use modular arithmetic to show that the sum of the divisors of n, $s(n)$ is congruent to n modulo 9. Indeed, if $n = 10^k a_j + 10^{k-1}a_{k-1} + \dots 10a_1 + a_0$, then since $10^j \equiv 1^j \equiv 1 \bmod 9$, then

$$n = 10^k a_k + 10^{k-1}a_{k-1} + \dots + 10a_1 + a_0 \equiv a_k + a_{k-1} + \dots + a_1 + a_0 = s(n) \bmod 9.$$

Just as when working in the real numbers one of our priorities is to solve linear algebraic equations for a variable, we're also interested in solving similar equations working in mods. To do so, we need to introduce the concept of multiplicative inverses.

If we were asked to solve the equation $2x = 6$, we would probably try to get rid of the 2 in front of the x. We can accomplish this by multiplying by $\frac{1}{2}$, which is the *multiplicative inverse* of 2 (i.e. the number that, when multiplied with 2, results in 1). Though we may not have a concept of $\frac{1}{2}$ in mods, we can still sometimes find multiplicative inverses for numbers.

Multiplicative Inverses

- Which numbers have multiplicative inverses in mod 3? mod 5? mod 11? mod p for prime p?
- Which numbers have multiplicative inverses in mod 4? mod 6? mod 10? mod 15? Do you notice anything these numbers have in common? (Hint: Look at the numbers with multiplicative inverses in relation to the mod in question)
- If a has a multiplicative inverse x in mod m, we write $ax \equiv 1 \pmod m$. Rewrite this as an *equation* (not a congruence) in the style of the division algorithm.
- Rearrange your equation from the previous part so that the constant (i.e. the remainder) is on one side and everything else is on the other side. Does this equation look familiar? What do we know about equations of this form?
- Conjecture when a number a has a multiplicative inverse in mod m. Use facts we have learned about equations of the particular form to prove your conjecture.

Lemma 2. Let a and b be relatively prime positive integers. Then $a, 2a, 3a, \dots, (b-1)a$ consists of different nonzero remainders modulo b.

Proof. Suppose that $ia \equiv ja \bmod b$. Since $(a, b) = 1$, then $i \equiv j \bmod b$. But the numbers $a, 2a, \dots, (b-1)a$ are all of the form ia with $1 \leq i \leq b-1$. Therefore, if $i \equiv j \bmod b$, then $i = j$. Now suppose that $ia \equiv 0 \bmod p$. Then $i \equiv 0 \bmod p$. This is impossible when $1 \leq i \leq b-1$. Therefore none of the numbers have remainder 0.

□

Reminder. When you're working with a problem and not sure what mod to use, look at what numbers appear in the problem. Often using one of these numbers or something close will be helpful.

5 Euler's Totient Function

Definition 6. For a positive integer n, we define $\phi(n)$ to be the number of positive integers that are $\leq n$ that are relatively prime to n. This function is called Euler's ϕ function or Euler's totient function.

For a prime p, it is easy to calculate $\phi(p)$. Indeed, all positive integers less than p are relatively prime to p, so $\phi(p) = p - 1$.

For a prime power p^α, it's also relatively easy to calculate. Consider all numbers between 1 and p^α (including both endpoints). The only numbers that are not relatively prime to p^α are the multiples of p. But the number of multiples of p in that range is $p^\alpha/p = p^{\alpha-1}$. Therefore

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha\left(1 - \frac{1}{p}\right).$$

For the product of two primes pq we have that if you're not relatively prime to pq, you must have be a multiple of p or a multiple of q. Using inclusion-exclusion we get

$$\phi(pq) = pq - \frac{pq}{p} - \frac{pq}{q} + \frac{pq}{pq} = pq - p - q + 1 = (p-1)(q-1) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

Let's find a general formula for $\phi(n)$ when $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Consider all numbers up to n. Then to not be relatively prime to n, you must be either a multiple of p_1 or p_2 or p_3 or $\dots$ p_r. By inclusion-exclusion we get

$$\begin{aligned}\phi(n) &= n - \frac{n}{p_1} - \frac{n}{p_2} - \cdots - \frac{n}{p_r} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \cdots + \frac{n}{p_{r-1}p_r} - \frac{n}{p_1p_2p_3} + \cdots + (-1)^r \frac{n}{p_1p_2\cdots p_r} \\ &= n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_r} + \frac{1}{p_1p_2} + \frac{1}{p_1p_3} + \cdots + \frac{1}{p_{r-1}p_r} - \frac{1}{p_1p_2p_3} + \cdots + (-1)^r \frac{1}{p_1p_2\cdots p_r}\right).\end{aligned}$$

where we consider all products of two primes p_ip_j, all products of three primes, of four primes, and so on. But since every k-fold product appears exactly once to the sign $(-1)^k$, that is $\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$. Therefore

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)\cdots p_r^{\alpha_r - 1}(p_r - 1). \tag{1}$$

A more compact way of writing the formula is

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

Theorem 6. Let a and b be relatively prime, then $phi(ab) = \phi(a)\phi(b)$

Proof. We arrange the numbers 1 to ab in an $a \times b$ array:

$$\begin{array}{cccc} 1 & 2 & \cdots & a \\ a+1 & a+2 & \cdots & 2a \\ \vdots & \vdots & \vdots & \vdots \\ a(b-1)+1 & a(b-1)+2 & \cdots & ab \end{array}$$

By definition, there are $\phi(ab)$ numbers relatively prime to ab in this array.

Next, note that there are $\phi(a)$ columns containing numbers relatively prime to a. Why? We know there are $\phi(a)$ numbers in the first row that are relatively prime to a (from the definition of the totient function). If $\gcd(a, c) = 1$, we know that $\gcd(ak + c, a) = 1$ for any integer k since $\gcd(ak + c, a) = \gcd(a, ak + c - ak) = \gcd(a, c)$ by the Euclidean algorithm.

Next, note that in any given column, each possible remainder upon division by b is represented exactly once. Why? Any two elements in a given column are of the form $ak_1 + c$ and $ak_2 + c$ for some integers $0 \le k_1, k_2 < b$ and $0 \le c < a$. Then if $ak_1 + c \equiv ak_2 + c \pmod b$, we know $ak_1 \equiv ak_2 \pmod b$ and thus since $\gcd(a, b) = 1$, $k_1 \equiv k_2 \pmod b$ by cancellation theorem. However, since all the k are distinct mod b, this means the $ak + c$ must be distinct as well. By the same logic as with a (that is $\gcd(b, c) = 1$ then $\gcd(bk + c, b) = 1$), this means any given column contains exactly $\phi(b)$ numbers relatively prime to b.

Notice that the numbers relatively prime to ab are exactly those that are relatively prime to both a and b. Since we know in each column there are $\phi(b)$ numbers relatively prime to b, and of those columns, $\phi(a)$ of them are relatively prime to a, this implies there are $\phi(a)\phi(b)$ numbers in the table relatively prime to ab. But we already know this is counted by $\phi(ab)$, so we have $\phi(ab) = \phi(a)\phi(b)$ as desired.

□

Remark 7. One can also prove Theorem 6 using the formula for $\phi(n)$ in (1). Alternatively, one can prove the formula for $\phi(n)$ using this theorem, because given $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Then repeatedly applying that $\phi(ab) = \phi(a)\phi(b)$ for $(a, b) = 1$ yields

$$\begin{aligned}
\phi(n) &= \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_{r-1}^{\alpha_{r-1}})\phi(p_r^{\alpha_r}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_r^{\alpha_r}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)
\end{aligned}$$

Example Consider $n = 693 = 3^2 \cdot 7 \cdot 11$. By our formula,

$$\begin{aligned}
\phi(693) &= 693\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right) \\
&= 693 - \frac{693}{3} - \frac{693}{7} - \frac{693}{11} + \frac{693}{3 \cdot 7} + \frac{693}{3 \cdot 11} + \frac{693}{7 \cdot 11} - \frac{693}{3 \cdot 7 \cdot 11}
\end{aligned}$$

Does this make sense? How many multiples of 3 are there that are less than or equal to 693? 231; multiples of 7? 99; multiples of 11? 63; multiples of 21? 33; multiples of 33? 21; multiples of 77? 9; multiples of 231? 3. So by the principle of inclusion-exclusion

$$\phi(693) = 693 - 231 - 99 - 63 + 33 + 21 + 9 - 3 = 360$$

which matches with

$$\phi(693) = 693 \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{10}{11} = 360.$$

Example Find the sum of all positive rational numbers that are less than 10 and that have denominator 30 when in lowest terms.

In order for a fraction to have denominator 30 when in lowest terms, the numerator must be relatively prime to 30. We know that $\phi(30) = 30 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$, so there are 8 numbers relatively prime to 30 that are less than 30.

Note that if $1 \leq k < n$ is relatively prime to n, so is $n - k$. This is because any common divisor d of n and k must divide $n - k$, and similarly any common divisor d of n and $n - k$ must divide $n - (n - k) = k$. This means numbers relatively prime to 30 come in pairs of the form $(m, 30 - m)$. This is convenient since

$$\frac{m}{30} + \frac{30 - m}{30} = \frac{30}{30} = 1.$$

This tells us the sum of the fractions less than 1 is 4.

Note that if $\frac{m}{30}$ is in lowest terms, then so is $\frac{m+30k}{30}$ for all integers 30. Thus we can add 1 to each of our fractions between 0 and 1 to get another fraction meeting our criteria between 1 and 2. We can add 1 to each of these to get fractions meeting our criteria between 2 and 3. This pattern continues. Thus, we have ten 4's contributed (one for 0-1, one for 1-2, and so on till 9-10) and each number 1 to 9 gets contributed eight times (since there are 8 fractions between 0 and 1, 8 between 1 and 2, etc.) Thus our final result is

$$4 \cdot 10 + 8 \cdot (1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9) = 400.$$

□

---

6 Fermat, Euler, Wilson

Theorem 8 (Fermat's Little Theorem)**.** For p prime, $a^p \equiv a \pmod{p}$. Alternatively, if $\gcd(a,p) = 1, a^{p-1} \equiv 1 \pmod{p}$.

Proof. We'll look at two cases: the zero case and the non-zero case. If $a \equiv 0 \pmod{p}$, then clearly $0^p \equiv 0 \pmod{p}$ and we're done.
Otherwise, a is non-zero, which means $\gcd(a,p) = 1$. Recall that the cancellation theorem tells us that if $\gcd(a,p) = 1$, then $ax \equiv ay \pmod{p}$ implies $x \equiv y \pmod{p}$. This tells us that $a, 2a, 3a, \ldots, (p-1)a$ must be distinct mod p. This tells us that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$
$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$$

Since $(p-1)!$ is relatively prime to p, we apply cancellation theorem to yield $a^{p-1} \equiv 1 \pmod{p}$ or $a^p \equiv a \pmod{p}$ as desired.

Alternative Proof. Let's prove it by induction. It's clearly true for $a = 0$ and $a = 1$ since $0^p = 0$ and $1^p = 1$. Now, suppose that it's true for some a. Then we want to prove it for $(a+1)^p$. By the Binomial Theorem we have

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + 1.$$

Consider i such that $1 \leq i \leq p-1$. We have $\binom{p}{i} = \frac{p!}{i!(p-1)!}$. Since $1 \leq i \leq p-1$, then $i!$ does not divide p. Since $1 \leq i \leq p-1$, then $1 \leq (p-i) \leq p-1$, so $(p-i)!$ does not divide p. But $\binom{p}{i}$ is an integer with a p factor in the numerator and no p factor in the denominator. Therefore $p|\binom{p}{i}$ and hence $\binom{p}{i} \equiv 0 \bmod p$. Using the induction hypothesis, we have $a^p \equiv a \bmod p$. Therefore

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \bmod p.$$

The proof is complete.

□

The contrapositive here gives a novel way to check the primeness of a number n. That is, if $a^n \not\equiv a \pmod{n}$, we know n is not prime. So given some large n, is $2^n \not\equiv 2 \pmod{n}$ then n is not prime.

Example. $2^{15} \equiv 256 \cdot 128 \equiv 1 \cdot 8 \equiv 8 \pmod{15}$ so 15 is not prime.

Note. If $2^n \equiv 2 \pmod{n}$, this doesn't guarantee n is prime (but it "probably" is). Numbers that satisfy this property are called "industrial grade primes."

Well that was nice. But the result only helps with prime modulae. Can we generalize this somehow?

Theorem 9 (Euler's Theorem)**.** If $\gcd(a,m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m)$ is the Totient Function.

Remark 10. In the case that m is prime, this is simply Fermat's Little Theorem.

Proof. Let $R_m = \{r_1, r_2, \ldots, r_k\}$ be the set of numbers relatively prime to m. This means $\phi(m) = k$. Since the r_i are distinct, the ar_i must be distinct mod m (easy to show by contrapositive). Since $(a,m) = 1$ and $(r_i, m) = 1$, $(ar_i, m) = 1$. By Euclidean Alg, this means

$$1 = \gcd(ar_i, m) = \gcd(m, ar_i \pmod{m})$$

So we have just permuted the elements of R_m. That is $\{ar_1, ar_2, \ldots, ar_k\} \equiv \{r_1, \ldots, r_k\} \pmod{m}$. So we can take the product of these sets to yield

$$(ar_1)(ar_2)\cdots(ar_k) \equiv r_1 r_2 \cdots r_k \pmod{m}$$
$$a^k r_1 r_2 \cdots r_k \equiv r_1 r_2 \cdots r_k \pmod{m}$$
$$a^k \equiv 1 \pmod{m}$$
$$a^{\phi(m)} \equiv 1 \pmod{m}$$

and we're done.

□

Theorem 11 (Wilson's Theorem)**.** For p prime, $(p-1)! \equiv -1 \pmod{p}$.

Proof. Let p be prime. Note that this means $1, 2, \ldots, p-1$ have multiplicative inverses in mod p. So everything will cancel except the numbers that are their own multiplicative inverses. These numbers are 1 and $p-1$ (recall CE4 from Week 1 Day 4). Since $p-1 \equiv -1 \pmod{p}$, we have

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$$

as desired.

Alternative Proof: Consider the number of permutations on $A = \{1, 2, \ldots, p\}$. On the one hand, the number is $p!$. On the other hand, we can think of a permutation on A as a function $f : A \to A$ that is onto. The number of functions $g : A \to A$ is p^p (for each input, we have p possible inputs). To find the onto functions, we have to remove whichever ones are not onto. Therefore, we must remove those that miss at least 1 value. There are $\binom{p}{1}$ ways of choosing the missed value and $(p-1)^p$ functions missing that particular value (for each input, we have $p-1$ possibilities). But when we remove all of these functions, we took out some too many times, indeed, any function that misses at least 2 values was over counted. So we have to add it back in. We get $\binom{p}{2}(p-2)^p$ such functions. We continue in this fashion using inclusion-exclusion to get the formula

$$p! = \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^p.$$

Now divide by p and analyze modulo p:

$$\begin{aligned}(p-1)! &= \frac{1}{p} \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^p = \sum_{k=0}^{p} (-1)^k \frac{(p-1)!}{k!(p-k)!} (p-k)^p \\ &\equiv (-1)^p \sum_{k=1}^{p-1} (-1)^k \frac{(p-1)!}{k!(p-k)!} k^n \bmod p. \end{aligned} \tag{2}$$

Now

$$\begin{aligned} k!(p-k)! &\equiv k(-1)^{k-1}(p-(k-1))(p-(k-2)) \cdots (p-1)(p-k)! \\ &\equiv k(-1)^{k-1}(p-1)! \bmod p. \end{aligned} \tag{3}$$

Therefore, from (2) and (3), we get

$$(p-1)! \equiv (-1)^p \sum_{k=1}^{p-1} (-1) \frac{(p-1)!}{k(p-1)!} k^p \equiv \sum_{k=1}^{p-1} k^{p-1} \bmod p.$$

From Fermat's Little Theorem, $k^{p-1} \equiv 1 \bmod p$. Therefore, the inner sum consists of $p-1$ ones and the proof is complete.

□

7 Diophantine Equations and Pythagorean Triples

Definition 7. A *Diophantine equation* is an algebraic equation whose coefficients and solutions are to be integer numbers.

For example: Find all positive integers a, b, c such that $a^2 + b^2 = c^2$. The triples (a, b, c) of positive integers satisfying $a^2 + b^2 = c^2$ are known as Pythagorean triples. The most famous one is $3^2 + 4^2 = 5^2$. Let's find a formula to generate all of them.

First note that if $\gcd(a,b,c) = d$ and $a^2 + b^2 = c^2$, then $\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = \left(\frac{c}{d}\right)^2$. We can therefore focus on solving the equation when $\gcd(a,b,c) = 1$ (since we can reduce any other triple to one with $\gcd(a,b,c) = 1$). These triples are called primitive triples.

Suppose $(a,b,c) = 1$ and $a^2 + b^2 = c^2$. Suppose $(a,b) = d$, then since $c^2 = a^2 + b^2$, we have $(a,b,c) = d$. This implies $d = 1$. Similarly, $(a,c) = 1 = (b,c)$. Since $(a,b) = 1$, they can't both be even. Suppose they are both odd, then a^2 and b^2 have remainder 1 when divided by 4, so c^2 has remainder 2. But there is no square that has remainder 2 when dividing by 4. Therefore one of a and b is even and the other is odd. Without loss of generality, suppose b is even. Since $a^2 + b^2 = c^2$, then $a^2 = (c-b)(c+b)$.

Now $(c-b, c+b) = (c+b, 2b)$. Since c is odd and b is even, then $c+b$ is odd. Therefore $(c+b, 2) = 1$. Therefore $(c+b, 2b) = (c+b, b) = (c, b) = 1$. Therefore $c-b$ and $c+b$ are relatively prime. But $(c-b)(c+b) = a^2$. By the Fundamental Theorem of Arithmetic, $c-b$ and $c+b$ both have to be squares that are relatively prime to each other. Therefore

$$c - b = u^2 \qquad c + b = v^2$$

Then we can solve for c and b and get

$$c = \frac{u^2 + v^2}{2} \qquad b = \frac{v^2 - u^2}{2},$$

where u and v are any odd positive integers that are relatively prime to each other. We then get that $a = \sqrt{(c-b)(c+b)} = uv$.

Therefore the Pythagorean triples are all of the form

$$\left(uvk, \frac{v^2 - u^2}{2}k, \frac{u^2 + v^2}{2}k\right),$$

where u, v are relatively prime odd integers and k is any positive integer. We can also swap a and b.

8 Linear Diophantine Equations

Linear Diophantine equations are equations like $ax + by = c$, where a, b, c are integers and we are only interested in solutions such that x and y are integers.

Big Question 1. Given some integers a, b for what integers c do there exist solutions to $ax + by = c$?

(a) What is the smallest positive integer d such that we can write $mx_0 + ny_0 = d$ for some integers x_0 and y_0?

(b) Do there exist x_1, y_1 such that $mx_1 + ny_1 = kd$ for an arbitrary integer k? If so, write x_1 and y_1 in terms of x_0 and y_0. If not, provide a counterexample and explain.

(c) Consider ℓ such that $d \nmid \ell$. Do there exist x_2, y_2 such that $mx_2 + ny_2 = \ell$? If so, write x_1 and y_1 in terms of x_0 and y_0. If not, provide a counterexample and explain.

(d) Based on what you found in parts b and c, when do we have a solution to the equation $mx + ny = z$ (where m, n, z are given integer values and x and y must be integers)?

Big Question 2. If there is a solution to an equation $ax + by = c$, how do we find it?

Big Question 3. Can there be multiple solutions to an equation $ax + by = c$? If so, how many are there and how do we find all of them?

(a) Consider the equation $2x + 3y = 1$. Find at least five (x, y) pairs that are solutions to this equation. Is there any limit to the number of solution pairs we can find?

(b) Do you see some pattern that relates your solutions from part a to one another? Hypothesize a general form for solutions to $ax + by = 1$ given that (x_0, y_0) is one solution (you may either write this symbolically or describe in words).

(c) Check your hypothesis from part b by looking at solutions to $3x + 5y = 1$ and $4x + 15y = 1$.

(d) Check your hypothesis from part b by looking at solutions to $2x + 3y = 4$ and $2x + 3y = 6$.

(e) What about the equations $2x+4y = 2$ or $6x+15y = 3$? Find at least five (x, y) pairs that are solutions to each equation. What is different here from the equations we dealt with before? How can we modify our hypothesis from part b to account for this difference?

(f) Suppose $ax + by = c$ is a linear diophantine equation with one solution (x_0, y_0). Give a general form for all solutions to the equation (you may either write this symbolically or describe in words).

Theorem 12. Let a, b, c be integers. Then the equation $ax + by = c$ has solutions in integers (x, y) if and only if $\gcd(a, b)|c$. In this case the equation has infinitely many solutions in ordered pairs of integer numbers. In fact, if (x_0, y_0) is an initial solution, then all solutions may be written like this:

$$(x, y) = \left(x_0 + \frac{kb}{\gcd(a, b)}, y_0 - \frac{ka}{\gcd(a, b)} \right),$$

where here k ranges through all integer numbers.

Remark 13. In the case of $\gcd(a, b) = 1$, solutions are parametrized $(x_0 + kb, y_0 - ka)$.

9 Chicken McNugget Theorem

We'll now discuss something colloquially referred to as the "Chicken McNugget Theorem." The supposed story is that McDonald's used to sell Chicken McNuggets in two different size offerings: 9 piece boxes and 20 piece boxes. Someone wondered what the largest number of Chicken McNuggets you couldn't order was (assuming no special orders or throwing away/eating McNuggets). The Chicken McNugget Theorem generalized and answered this question.

Notice that this is a bit different from the equations we have been discussing in that in this case, x and y must be nonnegative (i.e. we can't order negative boxes of McNuggets). Putting this in mathematical form, we have:

Theorem 14. If $\gcd(m, n) = 1$, the greatest integer that cannot be written in the form $mx + ny$ for *nonnegative* integers x, y is $mn - m - n$.

We will prove a stronger version of this theorem. To do so, we'll need to use the "we should name this" lemma:

Lemma 3. Let a and b be relatively prime positive integers. Then $a, 2a, 3a, \ldots, (b-1)a$ consists of different nonzero remainders modulo b.

Theorem 15 (Chicken McNugget Theorem)**.** For a, b relatively prime, there exists a maximum M such that there is no nonnegative integers x, y satisfying $ax + by = M$, and for any $n > M$, there exists nonnegative integers x, y such that $ax + by = n$. In fact $M = ab - a - b = (a - 1)(b - 1) - 1$ and the number of positive integers that don't have a linear representation of the form $ax + by$ with nonnegative integers x, y is $\frac{(a-1)(b-1)}{2}$.

Proof. One of a, b must be the maximum, so without loss of generality suppose $a > b$ (if $a = b$, then $a = b = 1$ to be able to be relatively prime and the statement is obvious). Consider the following table:

$$\begin{array}{rrrrrr}
0 & b & 2b & 3b & 4b & \ldots \\
a & a+b & a+2b & a+3b & a+4b & \ldots \\
2a & 2a+b & 2a+2b & 2a+3b & a+4b & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(b-1)a & (b-1)a+b & (b-1)a+2b & (b-1)a+3b & (b-1)a+4b & \ldots
\end{array}$$

The first row consists of all numbers congruent to 0 mod$b$ which are "representable" (we'll say that n is representable if there exist nonnegative integers x, y such that $ax + by = n$). The second row are all the numbers congruent to a mod b that are representable, and so on. The smallest number that is congruent to $(b-1)a$ mod b that is representable is $(b-1)a$. Therefore $(b-1)a - b = ab - a - b = M$ is not representable. Now let's show that anything beyond M is representable. Suppose $n > M$. Note that the rows represent the remainders of $0, a, 2a, 3a, \ldots, (b-1)a$ mod b. But by the Lemma, we know this represent all possible remainders. Now let i be such that $n \equiv ia$ mod b. If $i = (b-1)$, then because $M \equiv (b-1)a$ mod b and $n > M$, then $n \geq M + b = (b-1)a$. Therefore $n = (b-1)a + kb$ for some nonnegative integer k and hence it's representable. Now suppose $i < b-1$. We know $n > M = (b-1)a - b$, but $(b-1-i) > 0$ since $i < b-1$ and $a > b$, therefore $(b-1-i)a - b > a - b > 0$, which implies that $n > ia$. Since $n \equiv ia$ mod b and $n > ia$, then $n = ia + kb$ for some positive integer k. But then n is representable. This completes the proof that there is an M, that $M = ab - a - b$.

Now let's count the number of non-representable numbers. There are no numbers that are 0 mod b that are non-representable. The numbers congruent to a mod b that are not representable are those that are positive and less than a. Suppose $a = kb + r$ for some $0 < r < b$, then we can choose $j = 0, 1, 2, \ldots, k-1$ and $bj + r$ is a number congruent to a mod b that is not representable. Note that there are k numbers and that k is the quotient of a/b. This is the largest integer less than or equal to a/b. We denote this by $\left\lfloor \frac{a}{b} \right\rfloor$. Analogously we can show that the number of non-representable numbers is

$$S = \left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{2a}{b} \right\rfloor + \left\lfloor \frac{3a}{b} \right\rfloor + \ldots + \left\lfloor \frac{(b-1)a}{b} \right\rfloor.$$

Now note that $\left\lfloor \frac{ia}{b} \right\rfloor = \frac{ia}{b} - \frac{r_i}{q}$, where $r_i \equiv ia$ mod b and $0 \leq r_i \leq b-1$. Therefore we can replace each term in the sum S and get

$$\begin{aligned} S &= \frac{a}{b} - \frac{r_1}{b} + \frac{2a}{b} - \frac{r_2}{b} + \ldots + \frac{(b-1)a}{b} - \frac{r_{b-1}a}{b} \\ &= \left(\frac{a}{b} + \frac{2a}{b} + \ldots + \frac{(b-1)a}{b} \right) - \left(\frac{r_1}{b} + \frac{r_2}{b} + \ldots + \frac{r_{b-1}a}{b} \right) \\ &= \frac{a}{b}\left(1 + 2 + \ldots + (b-1)\right) + \frac{1}{b}\left(1 + 2 + \ldots + (b-1)\right) \\ &= \frac{a(b-1) - (b-1)}{2} = \frac{(a-1)(b-1)}{2}. \end{aligned}$$

Note that we used that the remainders of $a, 2a, \ldots, (b-1)a$ are all different and all nonzero, so that means $r_1 + r_2 + \ldots + r_{b-1} = 1 + 2 + \ldots + (b-1) = \frac{(b-1)b}{2}$.

Alternative Proof. This is an alternative proof of the fact that the number of positive integers that don't have a linear representation of the form $ax + by$ with nonnegative integers x, y is $\frac{(a-1)(b-1)}{2}$. The number of positive integers that are not expressed in the form $am + nb$ is

$$\left\lfloor \frac{a}{b} \right\rfloor + \left\lfloor \frac{2a}{b} \right\rfloor + \left\lfloor \frac{3a}{b} \right\rfloor + \ldots + \left\lfloor \frac{(b-1)a}{b} \right\rfloor.$$

Consider the following figure for the case $a = 5, b = 7$: It turns out that $\left\lfloor \frac{ia}{b} \right\rfloor$ is the number of points with integer coordinates between the line $y = \frac{a}{b}x$ and the x-axis. Therefore the sum is the number of lattice points[1] inside the triangle. Since $(a, b) = 1$, there are no lattice points on the diagonal. Therefore, we can use symmetry to see that the total number of lattice points is the number of lattice points inside the rectangle over 2. But the number of lattice points inside the rectangle is $(a-1)(b-1)$.

□

[1]Points with integer coordinates

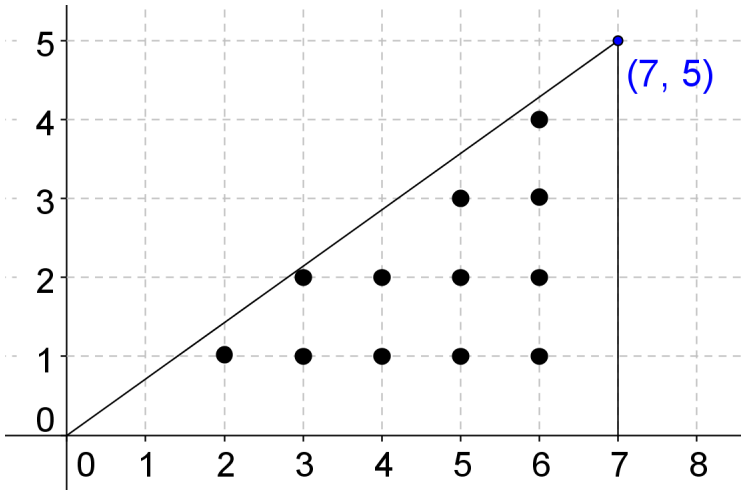

Figure 1: The points with integer coordinates below the line $y = \frac{5}{7}x$ when $0 < x < 7$.