Number Theory with python PROGRAMMING

Euler's Theorem

Lecture 7

Justin Stevens

Outline

1. Primes
   - Fermat's Little Theorem Challenge Problems
   - Pseudoprimes
   - Prime Number Theorem
   - Wilson's Theorem
2. Chinese Remainder Theorem
3. Euler's Totient Theorem

Fermat's Little Theorem Review

Theorem. If p is prime and a is an integer with $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Alternatively, for every integer a, $a^p \equiv a \pmod{p}$.

Challenge Problems

Example 1. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1$, $n \geq 1$

Example 2. (NIMO) Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p. Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.

IMO Problem

Example. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

Solution. I claim the answer is 1, therefore, every prime p divides a term in the sequence. For $p = 2$, $n = 1$ works and for $p = 3$, $n = 2$ works. By Fermat's Little Theorem for $n = p - 2$,

$$\begin{aligned} 6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) &\equiv 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \\ &\equiv 3 + 2 + 1 - 6 \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Therefore, for $p \neq 2, 3$, when $n = p - 2$, we have $p \mid 2^n + 3^n + 6^n - 1$.

NIMO Sum

Example. (NIMO) Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p. Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.

Solution. By FLT, $n^p \equiv n \pmod{p}$, so $\lfloor \frac{n^p}{p} \rfloor = \frac{n^p - n}{p}$ and the sum is

$$\sum_{k=1}^{p-2} \frac{k^p - k}{p} = \frac{1}{p} \sum_{k=1}^{p-2} (k^p - k) .$$

From the Binomial Theorem, $j^p + (p-j)^p \equiv 0 \pmod{p^2}$ for all j, so

$$\sum_{k=1}^{p-2} (k^p - k) \equiv 1^p - \sum_{k=1}^{p-2} k \equiv 1 - \frac{(p-2)(p-1)}{2} \equiv \frac{p(3-p)}{2} \pmod{p^2}.$$

Substituting $p = 2017$, $\frac{3-p}{2} \equiv \frac{-2014}{2} \equiv -1007 \equiv \boxed{1010} \pmod{p}$.

Pseudoprimes

Over 25 centuries ago, Chinese mathematicians believed n is prime iff $2^n \equiv 2 \pmod{n}$. The counterexample $n = 341$ was discovered in 1819.

Fermat's primality test says to pick a number a with $1 < a < p - 1$. If $a^{n-1} \not\equiv 1 \pmod{n}$, then we can conclude that a is composite. However, if the congruence holds, then we assign a high probability to n being prime.

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. Prove that if n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Mersenne Pseudoprimes

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. If n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof.

Since n is a base-2 pseudoprime, $2^{n-1} \equiv 1 \pmod{n}$, so $2^n \equiv 2 \pmod{n}$. Therefore, there exists an integer k with $2^n - 2 = kn$. Substituting, we have

$$\begin{aligned} 2^{M_n - 1} - 1 &= 2^{kn} - 1 \\ &= (2^n - 1)\left(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1\right) \\ &\equiv 0 \pmod{M_n}. \end{aligned}$$

Since n is composite, M_n is composite and the conclusion follows. □

Carmichael Numbers

A **Carmichael number** is an integer n that is a pseudoprime for every coprime base a. In other words, $a^{n-1} \equiv 1 \pmod{n}$ for every $\gcd(a, n) = 1$.

Example. Prove that 561 is a Carmichael number.

Proof. Factoring shows $561 = 3 \cdot 11 \cdot 17$. Therefore, for every a coprime to 3, 11, and 17, using Fermat's Little Theorem,

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Using these congruences, we see that

$$\begin{aligned} a^{560} &\equiv \left(a^2\right)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv \left(a^{10}\right)^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv \left(a^{16}\right)^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Therefore $a^{560} \equiv 1 \pmod{561}$ for all a relatively prime to 561.

Korselt's Criterion

The previous example establishes the intuition for the below theorem.

Theorem. (Korselt's Criterion) A number n is Carmichael if and only if $n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes and $p_i - 1 \mid n - 1$ for every $1 \leq i \leq r$.

Primality Tests

One way to test primality is trial division: if $d \nmid n$ for $2 \leq d \leq n-1$, then n is prime. This can be improved by observing that factors come in pairs:

$$48 = 1 \cdot 48 = 2 \cdot 24 = 3 \cdot 16 = 4 \cdot 16 = 6 \cdot 8.$$

The divisors flip around and repeat, so we only check $2 \leq d \leq \lfloor \sqrt{n} \rfloor$.

Theorem. (Eratosthenes) Write the numbers 1 to N in a grid. For all primes $p \leq \sqrt{N}$, cross out the multiples $2p, 3p, 4p, \cdots$ from. The numbers that remain are the primes less than N.

Example. Find all primes less than or equal to 100.

Example 3. Find all primes less than or equal to 100.

Solution. We show the completed grid using the Sieve of Eratosthenes:

	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	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

π Function

Definition. The number of primes less than or equal to a number n is defined as $\pi(n)$. For example, in our grid above, $\pi(100) = 25$.

Example 4. Find an exact formula for $\pi(n)$ if $p_1, p_2, \cdots, p_t$ are the primes $\leq \sqrt{n}$. *Hint:* Use Principle of Inclusion-Exclusion!

Exact Formula

Example. Find a formula for $\pi(n)$ if $p_1, p_2, \cdots, p_t$ are the primes $\leq \sqrt{n}$.

Solution. We start with n and subtract off the numbers $\leq n$ divisible by at least one p_i. We then add back the primes $p_1, p_2, \cdots, p_t$ and subtract 1. From Principle of Inclusion-Exclusion,

$$\pi(n) = n - \sum_i \lfloor \frac{n}{p_i} \rfloor + \sum_{i<j} \lfloor \frac{n}{p_i p_j} \rfloor - \sum_{i<j<k} \lfloor \frac{n}{p_i p_j p_k} \rfloor + \cdots + \pi\left(\sqrt{n}\right) - 1.$$

For small n, this gives a very compact way to compute $\pi(n)$. However, for larger values of n, computing the sum above isn't reasonable.

Theorem. (Prime Number Theorem) The number of primes less than or equal to n is asymptotic to $n/\ln(n)$. In other words,

$$\lim_{n \to \infty} \frac{\pi(n)}{n/\ln(n)} = 1.$$

History behind Theorem

We show a table of $\pi(n)$ for several powers of 10.

n	$\pi(n)$	$n/\ln(n)$
1000	168	145
10000	1229	1086
100000	9592	8686
1000000	78498	72382
10000000	664579	620420

In 1798 Legendre published the first significant conjecture on the size of $\pi(n)$ in his book "Essai sur la Théie des Nombres".

Tchebycheff made the first real progress towards proving the theorem in 1850 by showing that there exists constants $a \leq 1 \leq b$ with

$$a\,(n/\ln(n)) < \pi(n) < b\,(n/\ln(n))\,.$$

In 1896, Hadamard and de la Vallée Poussin completely proved the prime number theorem using Riemann's complex zeta function.

Other Estimates

While studying prime tables in 1791, Gauss came up with another estimate:

$$\pi(x) \approx \int_2^x \frac{dt}{\ln(t)} = \mathrm{Li}(x).$$

In his proof, de la Vallée Poussin proved that Gauss' Li function is always a better estimate than $n/\ln(n)$. He also showed that the best estimate of the form $n/(\ln(n) - a)$ is when $a = 1$. Consider the following table:

n	$\pi(n)$	Gauss' Li	$n/(\ln(n) - 1)$
1000	168	178	169
10000	1229	1246	1218
100000	9592	9630	9512
1000000	78498	78628	78030
10000000	664579	664918	661459

Table 1: Gauss' estimate of $\pi(n)$

Consequences of the Prime Number Theorem

One consequence is that the nth prime is approximately $p_n \approx n \ln(n)$.

Bertrand's Postulate states that there is always a prime between n and $2n$ for $n \geq 2$. He showed this for all integers up to 3 million by consider

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001, \cdots$$

This is a sequence of primes, each less than twice the predecessor.

Tchebycheff proved the result in 1852 using methods similar to the prime number theorem. In fact, the number of primes in the range is asymptotic to $n/\ln n$. "Proofs from the book" features an elementary method.

An unsolved problem is **Legendre's conjecture** that states there is always a prime between n^2 and $(n+1)^2$. This conjecture would imply that for any prime p, the gap between the next prime is in the order of $\sqrt{p}$.

Wilson's Theorem

Theorem. (Wilson) $(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.

Solution. When $p = 7$, $6! = 720 \equiv -1 \pmod{7}$. Alternatively,

$$6! = 1 \cdot (2 \cdot 4)\,(3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 \equiv -1 \pmod{7}.$$

We find groups of terms that multiply to 1 mod p. Observe that

$$x^2 \equiv 1 \mod p \iff (x-1)\,(x+1) \equiv 0 \mod p \iff x \equiv \pm 1 \mod p.$$

Since p is odd, this implies we can pair the inverses off into $(p-3)/2$ pairs, say $(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots (x_{(p-3)/2}, y_{(p-3)/2})$. Therefore,

$$\begin{aligned}(p-1)! &\equiv 1 \cdot (x_1 y_1)\,(x_2 y_2) \cdots \left[x_{(p-3)/2} y_{(p-3)/2}\right] \cdot (p-1) \pmod{p} \\ &\equiv 1 \cdot 1 \cdot 1 \cdots 1 \cdot (p-1) \pmod{p} \\ &\equiv -1 \pmod{p}.\end{aligned}$$

□

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod p$ iff $p \equiv 1 \pmod 4$.

Proof. If $x^2 \equiv -1 \pmod p$, then raising this to the power of $(p-1)/2$:

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

By Fermat's Little Theorem the LHS is 1, therefore $p \equiv 1 \pmod 4$.

By Wilson's Theorem, $(p-1)! \equiv -1 \pmod p$. Furthermore,

$$\begin{aligned}(p-1)! &= [1 \cdot (p-1)]\,[2 \cdot (p-2)] \cdots [(p-1)/2 \cdot (p+1)/2] \\ &\equiv (1 \cdot -1)\,(2 \cdot -2) \cdots [(p-1)/2 \cdot (-(p-1)/2))] \pmod p \\ &\equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p\end{aligned}$$

If $p \equiv 1 \pmod 4$, then $x = \left(\frac{p-1}{2}\right)!$ solves $x^2 \equiv -1 \pmod p$.

Outline

Linear Congruences Review

- The inverse of a mod m exists iff $\gcd(a, m) = 1$.
- If the Diophantine equation $ax + by = c$ has particular solution (x_0, y_0) and $d = \gcd(a, b)$, then the set of ordered integer solutions is

$$S = \left\{ \left(x_0 + \frac{b}{d} \cdot k, y_0 - \frac{a}{d} \cdot k \right) \,\middle|\, k \in \mathbb{Z} \right\}.$$

- If $ca \equiv cb \pmod{m}$, then $a \equiv b \pmod{m/d}$, where $d = \gcd(c, m)$.

Example

Example. Find all solutions to the congruence $18x \equiv 30 \pmod{42}$.

Solution. We can divide the congruence by $\gcd(18, 42) = 6$:

$$3x \equiv 5 \pmod{7}.$$

Listing numbers that are $5 \mod 7$, $5, \mathbf{12}, 19$, we see $x \equiv 4 \pmod{7}$:

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}.$$

Notice there are $d = \gcd(18, 42) = 6$ solutions to the congruence.

Solutions to General Congruence

Theorem. $ax \equiv b \pmod{m}$ has $d = \gcd(a, m)$ mutually incongruent solutions if $d \mid b$.

Let a particular solution to the Diophantine equation $ax + my = b$ have x value x_0. Then consider the d solutions

$$x_0,\, x_0 + \frac{m}{d},\, x_0 + 2\frac{m}{d},\, \cdots,\, x_0 + (d-1)\,\frac{m}{d}.$$

We begin by showing the solutions are unique. Assume for the sake of contradiction that two are the same. Therefore, there exists integers t_1 and t_2 such that $0 \leq t_1, t_2 \leq d - 1$ and

$$x_0 + t_1\frac{m}{d} \equiv x_0 + t_2\frac{m}{d} \pmod{m}.$$

Since $\gcd(\frac{m}{d}, m) = \frac{m}{d}$, we subtract x_0 and divide by $\frac{m}{d}$:

$$t_1 \equiv t_2 \pmod{d},$$

which is a contradiction. Therefore, the solutions are mutually incongruent.

Every Solution

Theorem. $ax \equiv b \pmod{m}$ has $d = \gcd(a, m)$ mutually incongruent solutions if $d \mid b$.

We now show that every number of the form $x_0 + t \cdot \frac{m}{d}$ is congruent to one of the d solutions above. Let $t = dq + r$, $0 \leq r \leq d - 1$ by the division algorithm. Therefore,

$$x_0 + t\frac{m}{d} = x_0 + (dq + r)\,\frac{m}{d} = x_0 + qm + r\frac{m}{d} \equiv x_0 + r \cdot \frac{m}{d} \pmod{m}.$$

Since $0 \leq r \leq d - 1$, this is a listed solution.

System of Linear Congruences

Since we solved a single linear congruence, we now consider the system:

$$a_1 x \equiv b_1 \mod m_1,\ a_2 x \equiv b_2 \mod m_2,\ \cdots,\ a_r x \equiv b_r \mod m_r.$$

Assume that the moduli m_k are pairwise relatively prime. The system will have no solution unless each individual congruence has a solution, therefore $d_k \mid b_k$ for each k, where $d_k = \gcd(a_k, m_k)$.

If this is the case, then d_k can be cancelled in the kth congruence to produce the system with the same solution:

$$a'_1 x \equiv b'_1 \mod n_1,\ a'_2 x \equiv b'_2 \mod n_2,\ \cdots,\ a'_r x \equiv b'_r \mod n_r.$$

Observe that $n_k = m_k/d_k$ and the moduli n_k are pairwise relatively prime. Furthermore, $\gcd(a'_i, n_i) = 1$, so the congruences have solutions

$$x \equiv c_1 \mod n_1,\ x \equiv c_2 \mod n_2,\ \cdots,\ x_r \equiv c_r \mod n_r.$$

Chinese Remainder Theorem

Theorem. Let $n_1, n_2, \cdots, n_r$ be pairwise relatively prime integers. Then

$$x \equiv c_1 \mod n_1,\ x \equiv c_2 \mod n_2,\ \cdots,\ x_r \equiv c_r \mod n_r$$

has a unique solution modulo $n_1 n_2 \cdots n_r$.

Proof. Let $N = n_1 n_2 \cdots n_r$ and $N_k = N/n_k = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$.

Since the moduli are pairwise relatively prime, $\gcd(N_k, n_k) = 1$ for every k. The congruence $N_k x_k \equiv 1 \pmod{n_k}$ then has a unique solution. Consider

$$\overline{x} = c_1 N_1 x_1 + c_2 N_2 x_2 + \cdots + c_r N_r x_r.$$

Observe that $N_k \equiv 0 \pmod{n_j}$ for $k \neq j$, so $\overline{x} \equiv c_j N_j x_j \equiv c_j \pmod{n_j}$. Therefore, $\overline{x}$ is a solution to our original system of congruences.

We now must prove that the solution is unique.

Uniqueness of Solution

Theorem. Let $n_1, n_2, \cdots, n_r$ be pairwise relatively prime integers. Then

$$x \equiv c_1 \mod n_1,\ x \equiv c_2 \mod n_2,\ \cdots,\ x_r \equiv c_r \mod n_r$$

has a unique solution modulo $n_1 n_2 \cdots n_r$.

Assume that x' is another integer that satisfies the system, so:

$$x' \equiv c_k \equiv \overline{x} \pmod{n_k}.$$

However, then $n_k \mid x' - \overline{x}$ for every k. Since the n_k are pairwise relatively prime, this implies $n_1 n_2 \cdots n_r \mid x' - \overline{x}$. In other words, $x' \equiv \overline{x} \pmod{N}$, contradiction. We have thus proven the Chinese Remainder Theorem

Sun-Tsu Puzzle

One example is due to the first-century Chinese mathematician Sun-Tsu:

Example. Solve the system of linear congruences

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7.$$

Solution. Using the notation from our proof, $N = 3 \cdot 5 \cdot 7 = 105$ and

$$N_1 = \frac{N}{3} = 35, \quad N_2 = \frac{N}{5} = 21, \quad N_3 = \frac{N}{7} = 15.$$

We furthermore see that the linear congruences

$$35x_1 \equiv 1 \pmod 3, \quad 21x_2 \equiv 1 \pmod 5, \quad 15x_3 \equiv 1 \pmod 7$$

are solved by $x_1 = 2, x_2 = 1$, and $x_3 = 1$. Therefore, a solution is

$$\overline{x} = c_1 N_1 x_1 + c_2 N_2 x_2 + c_3 N_3 x_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233.$$

Taking this modulo 105, our unique solution is $x \equiv 233 \equiv \mathbf{23} \pmod{105}$.

Least Common Multiple Puzzle

Example. Solve the system of linear congruences

$$x \equiv 6 \pmod 7, \qquad x \equiv 10 \pmod{11}, \quad x \equiv 12 \pmod{13}.$$

Solution. Observe that adding 1 to every congruence, we have

$$x + 1 \equiv 0 \pmod 7, \quad x + 1 \equiv 0 \pmod{11}, \quad x + 1 \equiv 0 \pmod{13}.$$

Therefore, we see that $7 \cdot 11 \cdot 13 \mid x + 1$, so $x \equiv \mathbf{1000} \pmod{1001}$.

Outline

Fermat's Omissions

Fermat occasionally omitted proofs of theorems he stated. When he proposed Fermat's Last Theorem, which claimed that there are no solutions to the diophantine equation $x^n + y^n = z^n$ for $n > 2$, he famously wrote

> *"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers.I have discovered a truly marvelous proof of this, which this margin is too narrow to contain." - Fermat in Arithmetica (1637)*

Fermat's Last Theorem was not finally proved until Andrew Wiles did so in 1993 (and later revised his proof in 1994): link to the proof.

Fermat also failed to prove his little theorem, therefore, a Swiss mathematician by the name of **Leonhard Euler** published a proof in 1736.

Euler continued to present other proofs of the theorem, and eventually generalized the problem in 1763 in his paper titled "Euler's theorem".

Euler's Totient Function

Definition. Define $\phi(m)$ to be the number of positive integers less than or equal to m that are relatively prime to m. For instance, $\phi(6) = 2$.

Example. Compute $\phi(24)$.

Solution. Factorizing $24 = 2^3 \cdot 3^1$, we find the number of integers that share a divisor with 24 using the **Principle of Inclusion-Exclusion**,

$$|\text{Mults of } 2| + |\text{Mults of } 3| - |\text{Mults of } 6| = 24/2 + 24/3 - 24/6 = 16.$$

Therefore, using complimentary counting, $\phi(24) = 24 - 16 = 8$. The numbers relatively prime to 24 are $1, 5, 7, 11, 13, 17, 19, 23$. Note that they come in pairs that sum to 24.

In general, for $n > 2$, $\phi(n)$ is even since $\gcd(n-a, n) = \gcd(a, n)$.

Multiplicative Function Review

Definition. A function f is **multiplicative** if whenever $\gcd(a, b) = 1$,

$$f(ab) = f(a)f(b).$$

Hence, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorzation of a number,

$$f(n) = f(p_1^{k_1})f(p_2^{k_2}) \cdots f(p_r^{k_r}).$$

Therefore, we only evaluate multiplicative functions up to prime powers.

Also, since $f(a \cdot 1) = f(a) \cdot f(1)$, we must have $f(1) = 1$ if $f \neq 0$.

Theorem. ϕ is a multiplicative function.

Visualization for $\phi(24) = \phi(3)\phi(8)$.

Mod 8

		0	**1**	2	**3**	4	**5**	6	**7**
Mod 3	0	24	9	18	3	12	21	6	15
	1	16	$\underline{1}$	10	$\underline{19}$	4	$\underline{13}$	22	$\underline{7}$
	2	8	$\underline{17}$	2	$\underline{11}$	20	$\underline{5}$	14	$\underline{23}$

Proof ϕ is multiplicative

For coprime m and n, we define the sets S_{mn} and $S_{(m,n)}$ by:

$$S_{mn} = \{a : \ 1 \leq a \leq mn \text{ and } \gcd(a, mn) = 1\}$$
$$S_{(m,n)} = \{(b, c) : \ 0 \leq b \leq m - 1 \text{ and } \gcd(b, m) = 1;$$
$$0 \leq c \leq n - 1 \text{ and } \gcd(c, n) = 1\}.$$

We prove there is a bijection from S_{mn} to $S_{(m,n)}$.

For an element $(b, c) \in S_{(m,n)}$, using the Chinese Remainder Theorem, there exists a unique solution to the linear congruences

$$x \equiv b \pmod{m}, \quad x \equiv c \pmod{n}$$

modulo mn, call it a. Furthermore, since b is relatively prime to m and c is relatively prime to n, $\gcd(a, mn) = 1$, therefore $a \in S_{mn}$.

Proof ϕ is multiplicative

$$\begin{aligned} S_{mn} &= \{a:\ 1 \le a \le mn \text{ and } \gcd(a, mn) = 1\} \\ S_{(m,n)} &= \{(b, c):\ 0 \le b \le m-1 \text{ and } \gcd(b, m) = 1; \\ &\qquad\qquad 0 \le c \le n-1 \text{ and } \gcd(c, n) = 1\}. \end{aligned}$$

If $a \in S_{mn}$, we divide a by m and n, respectively, to give remainders (b, c).

By the division algorithm, $0 \le b \le m-1$ and $0 \le c \le n-1$.

Furthermore, since a is relatively prime to mn, $\gcd(b, m) = 1$ and $\gcd(c, n) = 1$, so $(b, c) \in S_{(m,n)}$ and we have established our bijection.

By definition, $|S_{mn}| = \phi(mn)$ and $|S_{(m,n)}| = \phi(m)\phi(n)$. Therefore,

$$\phi(mn) = \phi(m)\phi(n).$$

Formula for ϕ

For a number n, if we write it as $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then by the multiplicative property of ϕ, $\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$.

For a prime p_i, the number of integers between 1 and $p_i^{e_i}$ inclusive that are multiples of p_i is $p_i^{e_i}/p_i = p_i^{e_i - 1}$. Therefore, using complimentary counting,

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

Substituting for each prime p_i, we arrive at the formula

$$\phi(n) = \prod_{i=1}^{k}\left(p_i^{e_i} - p_i^{e_i - 1}\right) = \prod_{i=1}^{k}\left[p_i^{e_i}\left(1 - \frac{1}{p_i}\right)\right] = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

For example, $\phi(24) = 24\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 8$.

Euler's Totient Theorem

Theorem. For coprime positive integers a and m, $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof. Let $r_1, r_2, \cdots, r_{\phi(m)}$ be a reduced residue system modulo m. I claim

$$\{ar_1, ar_2, \cdots, ar_{\phi(m)}\} \equiv \{r_1, r_2, \cdots, r_{\phi(m)}\} \pmod{m}.$$

Notice that every element of the left set is relatively prime to m since $\gcd(a, m) = 1$. Furthermore, if two distinct elements of the reduced residue set r_i and r_j are mapped to the same mod m element, then

$$ar_i \equiv ar_j \pmod{m} \implies r_i \equiv r_j \pmod{m}.$$

Since the sets are equivalent, their product must be as well:

$$a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{j=1}^{\phi(m)} r_j \pmod{m}.$$

Cancelling out the product since $\gcd(r_m, m) = 1$, $a^{\phi(m)} \equiv 1 \pmod{m}$.

Challenge Problems

Example 5. (AIME 1983) Let $a_n = 6^n + 8^n$. Determine the remainder on dividing a_{83} by 49.

Example 6. (Canada) Find the last 3 digits of $2003^{2002^{2001}}$.

AIME Problem

Example. (AIME 1983) Let $a_n = 6^n + 8^n$. Determine the remainder on dividing a_{83} by 49.

Solution. Since $\phi(49) = 42$, $6^{42} \equiv 1 \pmod{49}$ and $8^{42} \equiv 1 \pmod{49}$:

$$6^{83} + 8^{83} \equiv 6^{-1} + 8^{-1} \pmod{49}$$

We can compute $6^{-1} \equiv -8 \pmod{49}$ and $8^{-1} \equiv -6 \pmod{49}$, therefore

$$a_{83} \equiv -8 - 6 \equiv -14 \equiv \mathbf{35} \pmod{49}.$$

Alternatively, by distributing out the inverses,

$$6^{-1} + 8^{-1} \equiv 6^{-1}8^{-1}(8+6) \equiv 48^{-1} \cdot 14 \equiv -14 \equiv 35 \pmod{49}.$$

Canada Problem

Example. (Canada) Find the last 3 digits of $2003^{2002^{2001}}$.

Solution. We find the value mod 8 and find the value mod 125 then use the Chinese Remainder Theorem. First note that $\phi(8) = 4$, therefore,

$$2003^{2002^{2001}} \equiv 1 \pmod 8$$

since $4 \mid 2002^{2001}$. Next, we see that $\phi(125) = 100$, therefore we desire

$$2002^{2001} \equiv 2^{2001} \pmod{100}.$$

We find this value mod 4 and mod 25. Since $\phi(25) = 20$, we see

$$\begin{cases} 2^{2001} & \equiv 0 \pmod 4 \\ 2^{2001} & \equiv 2 \pmod{25} \end{cases} \implies 2^{2001} \equiv 52 \pmod{100}.$$

Canada Problem

Example. (Canada) Find the last 3 digits of $2003^{2002^{2001}}$.

We therefore have

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \equiv 3^{52} \pmod{125}.$$

By Euler's Totient Theorem, $3^{100} \equiv 1 \pmod{125}$, so

$$\left(3^{50}\right)^2 \equiv 1 \pmod{125} \implies 3^{50} \equiv \pm 1 \pmod{125}.$$

However, $3^{50} \equiv 9^{25} \equiv -1 \pmod{5}$, so $3^{50} \equiv -1 \pmod{125}$. Hence, $3^{52} \equiv -9 \equiv 116 \pmod{125}$. Combining these congruences we see

$$\begin{cases} 2003^{2002^{2001}} & \equiv 1 \pmod{8}, \\ 2003^{2002^{2001}} & \equiv 116 \pmod{125} \end{cases} \implies 2003^{2002^{2001}} \equiv \mathbf{241} \pmod{1000}.$$