More Computational Number Theory

Vidur Jasuja

November 2020

1 Chinese Remainder Theorem

You may have seen problems where you have some number of things and you try to divide them into groups of three but there are some number left over, and then into groups of four but there are some number left over, and then into groups of five but there are some number left over, and you're asked to find such a number. The Chinese Remainder Theorem is not a particularly useful theorem for computing mods themselves but it is important in solving such problems and is surprisingly powerful.

Theorem

Suppose $x_1, x_2, x_3, ..., x_n$ are some pairwise relatively prime integers, and $a_1, a_2, ..., a_n$ are some integers with $0 \leq a_i < x_i$.
Then the system of congruences

$$m \equiv a_1 \pmod{x_1}$$
$$m \equiv a_2 \pmod{x_2}$$
$$\cdots$$
$$m \equiv a_n \pmod{x_n}$$

Has exactly one integer solution m, where $0 \leq m < x_1x_2\cdots x_n$.

Proof

There are two parts to the proof. Firstly, we will show there is at most one integer in this range satisfying these congruences. Suppose there are two integers in this range, m_1 and m_2, satisfying the conditions. Then $a_i \mid (m_1 - m_2)$ for all i between 1 and 12, so then since the a_i's are pairwise relatively coprime, $a_1a_2a_3\cdots a_n \mid (m_1 - m_2)$. But given that $|m_1 - m_2|$ is at most $a_1a_2a_3\cdots a_n - 1$, then $m_1 - m_2 = 0$. Thus, we are done.

Now, we will show how to construct an integer, without guesswork, satisfying these conditions. Firstly, consider the first two congruences. Suppose b_1 is the inverse of $x_1 \pmod{x_2}$, and suppose that b_2 is the inverse of $x_2 \pmod{x_1}$. Then consider the integer $a_1b_2x_2 + a_2b_1x_1$.

$a_1b_2x_2 \equiv 0 \pmod{x_2}$, and $a_1b_2x_2 \equiv a_1 \cdot 1 \equiv a_1 \pmod{x_1}$. Also, $a_2b_1x_1 \equiv a_2 \cdot 1 \equiv a_2 \pmod{x_2}$, while $a_2b_1x_1 \equiv 0 \pmod{x_1}$. Thus, the sum of these two terms is congruent to $a_1 \pmod{x_1}$ and $a_2 \pmod{x_2}$, as desired.

Thus, we now have that there exists a unique integer c, $0 \leq c < x_1x_2$, such that $m \equiv c \pmod{x_1x_2}$. Now, we can apply the same process again with our congruences $\pmod{x_1x_2}$ and $\pmod{x_3}$, finding a unique integer which works $\pmod{x_1x_2x_3}$, and so on until we get an integer which works $\pmod{x_1x_2\cdots x_n}$.

2 Fermat's Little Theorem and Euler's Theorem

Theorem (Fermat's Little Theorem)

Suppose p is a prime. Then for all integers a, we have that $a^p \equiv a \pmod p$.

Proof

If $a \equiv 0 \pmod p$, then we know $a^p \equiv 0^p \equiv 0 \equiv a \pmod p$.

If $a \not\equiv 0 \pmod p$, then a and p are relatively prime. Thus, from last week, we know that the sets of integers $\{1, 2, 3, 4, \dots, p-1\}$ and $\{a, 2a, 3a, \dots, (p-1)a\}$ are the same.

Therefore, since the sets have the same elements but permuted $\pmod p$, the products of all of their elements are congruent $\pmod p$. Thus, we have

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

Which can be rearranged as

$$(p-1)! \cdot (a^{p-1} - 1) \equiv 0 \pmod p$$

But $(p-1)!$ is not divisible by p, so from Euclid's Lemma, we have that $a^{p-1} - 1 \equiv 0 \pmod p$. This means that $a^p - a \equiv 0 \pmod p$, as desired. We are done in either case.

However, note that the same argument does not apply to composite integers. What part of our proof would fail there?

Fortunately, there is a theorem which gives a similar result for composite integers (and is a generalization of FLT).

Definition (The Phi Function)

Given a positive integer n, $\varphi(n)$ is defined as the number of positive integers less than or equal to n which are also relatively prime to n.

Theorem (Euler's Theorem)

Suppose n is a positive integer, and a is an integer coprime to n. Then $a^{\varphi(n)} \equiv 1 \pmod n$.

Proof

Suppose $x_1, x_2, x_3, .., x_{\varphi(n)}$ are the $\varphi(n)$ integers less than or equal to n coprime to n. Since a is relatively prime to n, the numbers $ax_1, ax_2, ax_3, \dots, ax_{\varphi(n)}$ are all distinct modulo n. Moreover, they are all coprime to n. Thus, these two lists of $\varphi(n)$ integers are again simply permutations of each other.

Multiplying and subtracting, we find that $x_1 \cdot x_2 \cdots x_{\varphi(n)} \cdot (a^{\varphi(n)} - 1) \equiv 0 \pmod n$. But the product of the x_i's is coprime to n, so by the Fundamental Lemma, we are done.

This is a good theorem to have, but how can we compute $\varphi(n)$? There are three steps to deriving our formula.

Lemma 1

Suppose a, d are coprime. Then for any integer b, $a + db$ is coprime to b.

Proof

Suppose that $a + db$ and b have a common factor c. Then db has this factor c. Then $(a + db) - db = a$ has this factor c. This is a contradiction unless $c = 1$.

Lemma 2

If p is prime and k is positive, $\varphi(p^k) = p^k - p^{k-1} = (1 - \frac{1}{p})p^k$.

Proof

We will count the opposite; how many numbers less than or equal to p^k are not coprime to p^k. For a number to be not relatively prime to p^k, they must share a common prime factor, which must be p. Thus, there are $\frac{p^k}{p} = p^{k-1}$ numbers less than or equal to p^k not relatively prime to p^k, so there are $p^k - p^{k-1}$ which are.

Lemma 3

For relatively prime positive integers a and b, $\varphi(a)\varphi(b) = \varphi(ab)$.

Proof

Firstly, if an integer is relatively prime to ab, it must be relatively prime to a and b. The converse also holds; if there is some d which divides ab, but is coprime to a and b, this contradicts the Fundamental Lemma.

Now we count the number of positive integers less than or equal to a coprime to a, which is $\varphi(a)$, and the number of positive integers less than or equal to b coprime to b, which is $\varphi(b)$.

For each of these $\varphi(a)$ choices of a value modulo a and $\varphi(b)$ choices of a value modulo b, we find that there is one number between 1 and ab satisfying both of these congruences, and from Lemma 1 and the first paragraph of this proof, we find this number is coprime to ab. Furthermore, if we have a value modulo a or modulo b not coprime to a or b, respectively, the solution to these congruences is not coprime to either a or b, respectively, and is thus not coprime to ab.

What all of this tells us is that if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}) = p_1^{e_1}(1 - \frac{1}{p_1})p_2^{e_2}(1 - \frac{1}{p_2}) \cdots p_k^{e_k}(1 - \frac{1}{p_k})$.

$$\implies \varphi(n) = n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_k})$$

3 Problems

3.1 Wilson's Theorem

1. Wilson's Theorem says that for all primes p, we have that $(p-1)!+1 \equiv 0 \pmod{p}$.

   (a) Show that the case for 2 holds, and henceforth assume p is odd.

   (b) Show that 1 and $p-1$ are the only integers between 1 and $p-1$, inclusive, whose inverses are themselves.

   (c) Show that if b is the inverse of $a \pmod{p}$, then a is the inverse of $b \pmod{p}$.

   (d) Using the previous two parts, show that the product of all integers between 2 and $p-3$ is congruent to $1 \pmod{p}$. Following this, multiply in 1 and $p-1$ to finish the problem.

3.2 Squares congruent to -1

1. Suppose that $p \equiv 1 \pmod{4}$. Then, using Wilson's Theorem as well as the properties of mods, prove that $(\frac{p-1}{2}!)^2 \equiv -1 \pmod{p}$. (Hint: expand $(p-1)!$, and then manipulate your expression). This shows that if $p \equiv 1 \pmod{4}$, then there exists c such that $c^2 \equiv -1 \pmod{p}$.

2. Suppose that $p \equiv 3 \pmod{4}$. Then, using Fermat's Little Theorem as well as the properties as mods, show that there is no x for which $x^2+1 \equiv 0 \pmod{p}$.

3. Can you extend this to showing that p never divides x^2+y^2, save for when x and y are both multiples of p? (Hint: fractional mods)

3.3 Miscellaneous

1. Suppose I have $n < 60$ oranges. When I try to put them in baskets with 3 oranges each, I have 2 left over. When I try to put them in baskets with 4 each, I have 1 left over. When I try to put them in baskets with 5 oranges each, I have 3 left over. How many oranges do I have?

2. $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

3. Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7$.

4. Compute the remainder when 2^{100} is divided by 1000.

5. Show that there exists a sequence of 2020 consecutive composite integers.

6. Last year Isabella took 7 math tests and received 7 different scores, each an integer between 91 and 100, inclusive. After each test she noticed that the average of her test scores was an integer. Her score on the seventh test was 95. What was her score on the sixth test?

7. For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is $\{3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, \ldots\}$. Find the number of positive integers less than or equal to $10,000$ which are simultaneously 7-safe, 11-safe, and 13-safe.

8. One of Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that $133^5 + 110^5 + 84^5 + 27^5 = n^5$. Find the value of n.