Chinese Remainder Theorem

Dennis Chen, Kelin Zhu

NQT

The Chinese Remainder Theorem is a centerpiece of AIME and AMC Number Theory; many problems are unsolvable without invoking it and many more can be greatly simplified with it.

Chinese Remainder Theorem (abbreviated as CRT). For pairwise relatively prime positive integers $n_1, n_2, \ldots, n_k$, $a \bmod n_1 n_2 \cdots n_k$ uniquely determines $a \bmod n_i$ for $1 \le i \le k$, and vice versa.

1 Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic complements our knowledge from NPU-mods; it assists us in various operations such as finding GCD/LCM and p-adic valuation, which will be covered more in depth in NQV-Prime.

Fundamental Theorem of Arithmetic. Every number greater than 1 is either a prime or can be uniquely, up to order, expressed as a product of primes.

(You have probably heard of it or even discovered it on your own; the formal theorem reassures that you can assume such thing.)

If you are curious about the proof, you may check out `https://gowers.wordpress.com/2011/11/18/proving-the-fundamental-theorem-of-arithmetic/`.

Canonical Representation. The **canonical representation** of a positive integer n is of the form $p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$ for $p_1 < p_2 < \ldots < p_m, e_1, e_2 \ldots e_m > 1$

In conjunction with CRT, this means that we can evaluate any integer mod n by evaluating it mod $p_1^{e_1}, p_2^{e_2} \ldots$

2 Two Main Archetypes

CRT tells us that we can:

1. given an independent system of linear congruences, you can "stitch them together" to one linear congruence that encompasses all of the conditions. This is often used when you obtain two mod conditions that are disjoint into one big condition that is easier to work with. In particular, finding values satisfying two linear congruences is hard, but finding values satistfying one modular congruence means one simply has to work with an arithmetic sequence.

2. given a linear congruence, you can "take it apart" into an independent system of linear congruence that encompasses the original congruence, and solve them independently. This is often used to split up a residue mod a composite number into residues mod prime powers, that are usually much more

tolerable, and then using the previous to "put them back together" to find a exact value. For example, one might want to find the last three digits of a large number N. What one would do is find $N \pmod 8$ and $N \pmod{125}$, then combine them to find $N \pmod{1000}$.

Here is a straightforward example of the first archetype:

Example. Find a positive integer n that is less than or equal to 504, and leaves a remainder of 4 when divided by 7, 2 when divided by 8, and 1 when divided by 9.

Solution. First, notice that $504 = \operatorname{lcm}(7, 8, 9)$ and any two of $7, 8, 9$ are relatively prime, so we can apply CRT here. We can simplify the calculation significantly by first combining the first two congruences, and only then bringing the third into play. The first two congruences tells us that $n \equiv 18 \pmod{56}$. Combining this with $n \equiv 1 \pmod 9$, we can find that $n \equiv 298 \pmod{504}$, so our unique answer is **298**.

Remark: There are many tricks one can use to speed up the above computations. First, observe that $7 \equiv -1 \pmod 8$, and so $7k + 4$ would be equivalent to $4 - k$. After that, notice that $18 \equiv 0 \pmod 9$, so we are just looking for the inverse of 56 mod 9, multiplying it with 56 outside of modulus and adding 18.

These won't be universally applicable, but keep in mind that intuition in general modular arithmetics does carry over to solving CRT congruences, and you shouldn't completely neglect it because it's particularly useful in contests such as MATHCOUNTS and AMC 10/12, where computation speed is the main hurdler of difficulty.

The following special case that has a nice solution. You will be surprised at how often it pops up in mediocre-quality mock contests and MATHCOUNTS, in an attempt to trip up inexperienced contestants who will attempt to bash.

Example (Negative remainders). Find a positive integer n that is less than or equal to 504, and leaves a remainder of 5 when divided by 7, 6 when divided by 8, and 7 when divided by 9.

Solution. $5 \equiv -2 \pmod 7, 6 \equiv -2 \pmod 8, 7 \equiv -2 \pmod 9$. The answer is $504 - 2 =$ **502**.