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. For pairwise relatively prime positive integers $n_1, n_2, \ldots, n_k$, a mod $n_1 n_2 \cdots n_k$ uniquely determines a mod n_i for $1 \le i \le k$, and vice versa.

This might seem like a useless jumble of text at first, but the following few exemplar applications will decrypt its statement and show its power.

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 $N \pmod{1000}$.

1 Fundamental Theorem of Arithmetics

This will be explored in greater depth in the NQV-Prime unit, but it goes along really well with CRT and complements our knowledge from NPU-Mods, so I will include it.

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.

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

In conjunction with CRT, this means if a positive integer n is equal to $p_1^{e_1} p_2^{e_2} \ldots$ for distinct primes $p_1, p_2 \ldots$, we can evaluate any integer mod n by evaluating it mod $p_1^{e_1}, p_2^{e_2} \ldots$