Chinese Remainder Theorem

Dennis Chen, Kelin Zhu

NQU

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.

0.1 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 $p_1^{e_1}, p_2^{e_2} \ldots$

0.2 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 $N \pmod{1000}$.

1 Merging congruences

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**.

Here is a more bashy example on a recent AMC:

Example (AMC 10A 2020/24). Let n be the least positive integer greater than 1000 for which

$$\gcd(63, n + 120) = 21 \quad \text{and} \quad \gcd(n + 63, 120) = 60.$$

What is the sum of the digits of n?

A somewhat pedagogical and unrelated comment: the problem asks for the sum of the digits of n because otherwise you could game the problem by just trying all of the answer choices. In this case, the problem does not imply that finding the sum of the digits of n as opposed to finding n will solve the problem in a quicker or easier way. This sort of approach does humorously work sometimes, and is a tip for guessing.

Solution. Our gcd equations give us possible remainders of n when divided by 63 and 120, which clues us in to the Chinese Remainder Theorem. In particular, we know we are going to want to put them together into one big congruence, as $n > 1000$.

Note that $n + 120 \equiv 0 \pmod{21}$, or $n \equiv 6 \pmod{21}$, but also note that $n \not\equiv 6 \pmod{63}$. Thus $n \equiv 27 \pmod{63}$ or $n \equiv 48 \pmod{63}$. Similarly, $n \equiv 117 \pmod{120}$. This gives us two possible systems of congruences.

The first system is

$$\begin{aligned} n &\equiv 27 \pmod{63} \\ n &\equiv 117 \pmod{120}. \end{aligned}$$

Note that the factor of 3 is redundant in the second congruence, as this is equivalent to

$$n \equiv 0 \pmod 9$$

$$n \equiv 6 \pmod 7$$
$$n \equiv 3 \pmod 8$$
$$n \equiv 2 \pmod 5,$$

so it is equivalent to

$$n \equiv 27 \pmod{63}$$
$$n \equiv 37 \pmod{40}.$$

Note that we want to solve the system

$$n \equiv 63a + 27 \pmod{63}$$

$$n \equiv 63a + 27 \equiv 23a + 27 \equiv 37 \pmod{40}.$$

Now we just sensibly add multiples of 23 and pray that $23a + 30$ becomes divisible by 40. This occurs when $a = 30$, so

$$n \equiv 63a + 27 \equiv 63 \cdot 30 + 27 \equiv 1917 \pmod{2520}.$$

So the smallest n in this system is $n = 1917$.

To top it off, here is an actually relatively nice problem that combines the knowledge of CRT and divisibility.

Example (AIME I 2013/11). Ms. Math's kindergarten class has 16 registered students. The classroom has a very large number, N, of play blocks which satisfies the conditions:

(a) If 16, 15, or 14 students are present, then in each case all the blocks can be distributed in equal numbers to each student, and

(b) There are three integers $0 < x < y < z < 14$ such that when x, y, or z students are present and as much blocks as possible are evenly distributed, there are exactly three blocks left over.

Find the sum of the distinct prime divisors of the least possible value of N satisfying the above conditions.

Solution. N is a multiple of $16, 15$ and 14. This makes it a multiple of every positive integer under 14 other than $9, 11, 13$, which forces the values of x, y and z.

Let $N = \text{lcm}(14, 15, 16) \cdot n = 1680n$; we can then solve for the equivalences

$$1680n \equiv 3 \pmod 9 \longrightarrow n \equiv 2 \pmod 3$$
$$1680n \equiv 3 \pmod{11} \longrightarrow n \equiv 10 \pmod{11}$$
$$1680n \equiv 3 \pmod{13} \longrightarrow n \equiv 1 \pmod{13}$$

Noting $1 = 11 - 10 = 3 - 2$, we can quickly find that $n = 33k - 1$; it doesn't take much more work to find $k = 4$. 131 is prime, so our answer is $131 + 2 + 3 + 5 + 7 = \mathbf{148}$.

The difficulty in these problems often comes from computational intensity rather than actual ingenuity, and therefore, the best way to practice them is simply to bash frequently.

2 Splitting congruences

The second archetype is more interesting, more common on the latter end of AIME, and usually harder to spot. It also usually involves exponential NT knowledge.

Something that you will absolutely need to know for NT in general is Fermat's Little Theorem, which takes the following form:

Fermat's Little Theorem. Consider a prime p. For any integer a, $a^p \equiv a \pmod{p}$.

If we add the restriction that a and p are relatively prime, we can divide by a on both sides to achieve the following.

Fermat's Little Theorem, alternative. Consider a prime p. For relatively prime a, p, $a^{p-1} \equiv 1 \pmod{p}$.

Example (AIME I 2014/8). The positive integers N and N^2 both end in the same sequence of four digits $abcd$ when written in base 10, where digit a is not zero. Find the three-digit number abc.

Solution. Note that by the Chinese Remainder Theorem,

$$N^2 \equiv N \pmod{16}$$

$$N^2 \equiv N \pmod{625}.$$

This implies that

$$N(N-1) \equiv 0 \pmod{16}$$

$$N(N-1) \equiv 0 \pmod{625}.$$

Ignoring the restriction of $a \neq 0$, we can have $N \equiv 0, 1 \pmod{16}$ and $N \equiv 0, 1 \pmod{625}$, resulting in 4 overall systems of congruences to solve.

Obviously $N \equiv 0 \pmod{16}$ and $N \equiv 0 \pmod{625}$ leads to $N \equiv 0 \pmod{10000}$, and $N \equiv 1 \pmod{16}$ and $N \equiv 1 \pmod{625}$ leads to $N \equiv 1 \pmod{10000}$, so they aren't what we're looking for.

We try $N \equiv 1 \pmod{16}$ and $N \equiv 0 \pmod{625}$. To find the value of N that will make CRT Congruences work, we are trying to find $N \equiv 625n \pmod{625}$ such that $625n \equiv 1 \pmod{16}$. Note that $625n \equiv n \equiv 1 \pmod{16}$, implying that $n = 1$ will suffice, leaving us with $N \equiv 625 \pmod{16}$ and $N \equiv 625 \pmod{625}$, or $N \equiv 625 \pmod{10000}$. This has $a = 0$, so it isn't what we're looking for.

We now try $N \equiv 0 \pmod{16}$ and $N \equiv 1 \pmod{625}$. To find the value of N that will make CRT Congruences work, we are trying to find $N \equiv 625n + 1 \pmod{625}$ such that $625n + 1$ is divisible by 16. Note that $625n + 1 \equiv n + 1 \pmod{16}$, so $n = 15$ will suffice, leaving us with

$$N \equiv 16 \cdot 586 \equiv 9376 \pmod{16}$$

$$N \equiv 625 \cdot 15 + 1 \equiv 9376 \pmod{625},$$

or $N \equiv 9376 \pmod{10000}$. So the answer is **937**.

Example (AIME I 2018/11). Find the least positive integer n such that when 3ˆn is written in base 143, its two right-most digits in base 143 are 01.

Solution. We have that $3^n \equiv 1 \pmod{143^2}$, which we can split into $3^n \equiv 1 \pmod{11^2}$ and $3^n \equiv 1 \pmod{13^2}$.

The first congruence is easy to solve, as $3^5 = 2 \cdot 11^2 + 1$.

The second is more troublesome, but notice that $3^3 \equiv 1 \pmod 13$. We can try out numbers of the form $12k + 3$ (else, n won't even satisfy the mod 13 congruence!) until one works for 13^2, praying that k won't be large; fortunately, $k = 3$ satisfies the condition.

Our answer is therefore $\operatorname{lcm}(5, 39) = \mathbf{195}$.

Remark: This problem is included because it reveals a common disguise in NT: bases as a way to rephrase modular congruences. It often takes on more complex forms than the laughably thin veil in this problem.

If you're an expert Number Theorist, you might notice other ways to solve the second congruence. They are beyond the scope of this unit, but feel free to check the dedicated AoPS thread at https://artofproblemsolving.com/community/c5h1604138p9995346 nonetheless for alternative methods.

As the capstone of this "split into prime powers" idea, here is how the unique divisibility properties of primes solves an IMO problem in conjunction with CRT:

Example (IMO 2009/1). Let n be a positive integer and let $a_1, a_2, a_3, \ldots, a_k$ $(k \geq 2)$ be distinct integers in the set $1, 2, \ldots, n$ such that n divides $a_i(a_{i+1} - 1)$ for $i = 1, 2, \ldots, k - 1$. Prove that n does not divide $a_k(a_1 - 1)$.

Solution. For the sake of contradiction, suppose that n can divide $a_k(a_1 - 1)$.

Let p^e be a prime power factor of n such that p^{e+1} is not a factor of n. (In other words, $\nu_p(n) = e$)

If some a_j is a multiple of p^e. Then, $a_j - 1$ is relatively prime to it, hence a_{j-1} is also a multiple of it. Working circularly, all terms of the sequence a_i are multiples of p^e.

Similarly, if $a_j - 1$ is a multiple of p^e, then a_j is relatively prime to it, and we can get that all terms are equivalent to 1 mod p^e.

Iterating over all prime power factors of n, we find that all terms are congruent mod n by CRT, which cannot happen.

In Olympiad problems, CRT is mostly useful because it guarantees the existence of something. In the above example, the exact values of $a_1, a_2 \ldots$ are irrelevant; all that we need to know is that they are congruent mod n when they are supposed to be distinct.

3 Problems

Minimum is [TBD ♟]. Problems denoted with ♞ are required. (They still count towards the point total.)

> "There is no instance of a nation benefitting from prolonged warfare."
>
> Sun Tzu, The Art of War

[1 ♟] **Problem 1** Find the least positive integer n congruent to 4 modulo 11, 7 modulo 17 and 8 modulo 19. You are allowed to use a calculator. [1 ♟] **Problem 2 (MAST Diagnostic 2020)** How many integer values of $1 \leq x \leq 100$ makes $x^2 + 8x + 5$ divisible by 10?