The Chinese Remainder Theorem

Evan Chen
evanchen@mit.edu

February 3, 2015

> The Chinese Remainder Theorem is a "theorem" only in that it is useful and requires proof. When you ask a capable 15-year-old why an arithmetic progression with common difference 7 must contain multiples of 3, they will often say exactly the right thing.
>
> — Dominic Yeo, Eventually Almost Everywhere

This article, aimed at olympiad students, focuses on the application of the Chinese Remainder Theorem in mathematical olympiads.

§1 Warm-Up

Problem 1.1 (USAMO 2008/1)**.** Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1, \dots, k_n$, all strictly greater than 1, such that $k_0 k_1 \dots k_n - 1$ is the product of two consecutive integers.

§2 The Chinese Remainder Theorem

First let me write down what the formal statement of the Chinese Remainder Theorem.

Theorem 2.1 (Chinese Remainder Theorem)
Let $m_1, \dots, m_k$ be pairwise relatively prime positive integers, and let

$$M = m_1 \dots m_k.$$

Then for every k-tuple $(x_1, \dots, x_k)$ of integers, there is exactly one residue class $x \pmod M$ such that

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x &\equiv x_k \pmod{m_k}. \end{aligned}$$

As explained in the opening quote, the theorem above has no real substance. It really is just formalizing a piece of intuition[1] that you could easily have picked up on your own from doing enough problems. But that's not to say the theorem is useless – it is useful because the intuition behind it is useful. To see how versatile this notion is, we can phrase the theorem in the following ways.

[1] Muirhead and linearity of expectation are more examples of this kind of flavor.

Chinese Remainder Theorem A (Construction)

Given the x_i's and m_i's, there exists an x which simultaneously satisfies each

$$x \equiv x_i \pmod{m_i} \quad \text{for all } i.$$

In this perspective, we are given the m_i and want to build up an x. Note that the resulting x is probably **huge**, just because the number M is large and the answer is unique modulo M. Moreover there isn't an especially easy way to write down the value of x. In other words, this perspective talks about things we can't actually see. The pessimist might be disappointed now, but the optimist is overjoyed – **this perspective lets us access otherwise hard-to-reach numbers with properties we want**.

Somewhat related is the following.

Chinese Remainder Theorem B (Lifting)

If $x \equiv k \pmod{m_i}$ for every i, then we actually have $x \equiv k \pmod{M}$.

Note again that M is *huge*. Surprisingly, this is a good way to get size results: since M is often very large, x is often very large too.

Finally, to talk about things not-huge, we have the following.

Chinese Remainder Theorem C (Destruction)

To understand $x \pmod{M}$, we only need to understand $x \pmod{m_i}$ for every i. In particular, we can reduce any statement modulo M to a statement modulo each of its prime powers.

This means that given an M we can *reduce* the problem.

And no, these names are not standard. I made them up.

§3 Example Problems

As with any "vacuous" theorem, it's important that we *internalize* these ideas. The Chinese Remainder Theorem is a very natural, intuitive concept, and therefore it is used most effectively when we don't think explicitly about having to use it.

Let's look at some examples of how we can apply each of these perspectives. The key is that while the Chinese Remainder Theorem is *used* in all the problems, it is not really the key step to the solution; rather, it serves as a way for us to see what to do. It really ought to be called a "lemma", but blame history...

§3.1 Construction

Let's begin by looking at the warm-up problem.

Example 3.1 (USAMO 2008/1)

Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1, \ldots, k_n$, all strictly greater than 1, such that $k_0 k_1 \ldots k_n - 1$ is the product of two consecutive integers.

Proof. Essentially we are being asked to show that $t(t+1)+1 = k_0 \dots k_n$ can have arbitrarily many prime factors. Indeed, if it suffices to prove that for any n there exists a t such that $P(t) = t^2+t+1$ has more than $n+1$ prime divisors.

Now how do we go about getting that many prime divisors? We want to construct a t such that $P(t) \equiv 0 \pmod{p_i}$ for some n primes $p_0, \dots, p_n$. But for this, we just have to construct a t_i such that $P(t_i) \equiv 0 \pmod{p_i}$ for every i. Once that's done, the Chinese Remainder Theorem enables us to select at t such that $t \equiv t_i \pmod{p_i}$ for all i, meaning $P(t) \equiv P(t_i) \equiv 0 \pmod{p_i}$.

In other words, the problem just reduces to proving that there are infinitely many primes dividing some number of the form t^2+t+1. So, we've managed to eliminate almost all the structure of the problem before using the Chinese Remainder Theorem, leading us to this heart of the problem. And to prove this, we simply have to mimic Euclid's classical proof of the infinitude of primes. Assume for contradiction that $\mathcal{P}$ is a full set of primes. Take the product N of all primes in $\mathcal{P}$ and look at N^2+N+1. It cannot be divisible by any prime in $\mathcal{P}$, contradiction. □

Let's see an even more extreme example.

Example 3.2 (TSTST 2012/3)

Let $\mathbb{N}$ be the set of positive integers. Let $f : \mathbb{N} \to \mathbb{N}$ be a function satisfying the following two conditions:

(a) $f(m)$ and $f(n)$ are relatively prime whenever m and n are relatively prime.

(b) $n \le f(n) \le n + 2012$ for all n.

Prove that for any natural number n and any prime p, if p divides $f(n)$ then p divides n.

Proof. Fix n and p, and assume for contradiction $p \nmid n$.

The idea is that I will construct large integers N such that $f(N) = N$. Here is how: pick $2012 \cdot 2013$ distinct primes $q_{i,j} > n+p+2013$ for every $i = 1, \dots, 2012$ and $j = 0, \dots, 2012$, and use it to fill in the following table:

	$N+1$	$N+2$	$\dots$	$N+2012$
M	$q_{0,1}$	$q_{0,2}$	$\cdots$	$q_{0,2012}$
$M+1$	$q_{1,1}$	$q_{1,2}$	$\cdots$	$q_{1,2012}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$M+2012$	$q_{2012,1}$	$q_{2012,2}$	$\cdots$	$q_{2012,2012}$

.

By the Chinese Remainder Theorem, we can construct N such that $N+1 \equiv 0 \pmod{q_{i,1}}$ for every i, and similarly for $N+2$, and so on. Moreover, we can also tack on the condition $N \equiv 0 \pmod{p}$ and $N \equiv 1 \pmod{n}$. Notice that N cannot be divisible by any of the $q_{i,j}$'s, since the $q_{i,j}$'s are greater than 2012.

After we've chosen N, we can pick M such that $M \equiv 0 \pmod{q_{0,j}}$ for every j, and similarly $M+1 \equiv 0 \pmod{q_{1,j}}$, et cetera. Moreover, we can tack on the condition $M \equiv 1 \pmod{N}$.

What does this do? We claim that $f(N) = N$ now. Indeed, since $M \equiv 1 \pmod{N}$ we have $\gcd(M, N) = 1$. so $f(M)$ and $f(N)$ are relatively prime by the condition. But look at the table! The table tells us that $f(M)$ must have a common factor with each of $N+1, \dots, N+2012$. So the only possibility is that $f(N) = N$.

Now we're basically done. Since $N \equiv 1 \pmod{n}$, we have $\gcd(N, n) = 1$ and hence $1 = \gcd(f(N), f(n)) = \gcd(N, f(n))$. But $p \mid N$ and $p \mid f(n)$, contradiction. □

Notice how **grotesquely large** the numbers involved in the proof are. The size of M is on the order of

$$\prod_{i,j} q_{i,j} \cdot N > 2013^{2013^2}.$$

Playing with numbers that big seems obscene, but it solves the problem. That's the power of the Chinese Remainder Theorem; we can access large numbers we couldn't access otherwise. All you have to do is let go of your sense of decency! In the words of Paul Zeitz: **good, obedient boys and girls solve fewer problems than naughty and mischievous ones**.

§3.2 Lifting

Remember the remark about size? Let's see how it applies here.

Example 3.3 (Harder than USAMO 2014/6)

Prove that there is a constant $c > 0$ with the following property: If a, b, n are positive integers such that $\gcd(a + i, b + j) > 1$ for all $i, j \in \{0, 1, \dots n\}$, then

$$\min\{a, b\} > (cn)^n.$$

What's interesting about this problem? The hypothesis involves nothing but divisibilities. The conclusion involves nothing but size. How are these two things related? In general, we just don't know much about multiplicative structure, and that leads us to suspect that the solution involves the Chinese Remainder Theorem in its Lifting form: if we can show, for example, $a + i \equiv 0 \pmod{\text{something really big}}$, that would do the trick. We can see this running in the solution sketch below.

Sketch of Proof. The idea is as follows. We know for each $0 \le i, j \le n$, some prime divides both $a+i$ and $b+j$. Let's write down all the information we have in an $(N+1) \times (N+1)$ table in the obvious manner. Our table might look something like:

.	2	.	2	.	2	.	2	.	2	.
.	.	5	7	.	.	.	5	.	.	7
.	2	3	2	.	2	.	2	3	2	.
.	.	.	.	.	.	.	.	.	.	.
.	2	.	2	.	2	.	2	.	2	.
.	.	3	.	.	3	.	.	3	.	.
.	2	5	2	.	2	.	2	.	2	.
.	.	.	.	.	.	.	.	.	.	.
.	2	3	2	.	2	.	2	3	2	7
.	.	.	.	.	.	.	.	.	.	.
.	2	.	2	.	2	.	2	.	2	.

or something like that. Notice how the primes fill in a evenly spaced "subgrid". Thus a prime p takes up at most a fraction p^{-2} of the entire grid. But $\sum_p p^{-2}$ is not very big; in fact, it's less than $\frac{1}{2}$. What this means is that we'll run out of small primes very quickly, and the table will have a lot of big primes.

With enough calculations with $\sum \left\lceil \frac{n+1}{p} \right\rceil^2$, you can show that at least half the table consists of primes greater than $0.001n^2$. So some column must have at least half its entries as primes greater than $0.001n^2$. Hence $a+i$ is divisible by the product of all these primes which is greater than $(0.001n^2)^{n/2} = (cn)^n$. That's all there is to it! □

This problem was a USAMO #6, and it looked scary, but was it that bad? The ideas behind it are very natural: try to fill up a grid with primes, realize that there are not enough small primes, and then use CRT to connect this and get a size result.

§3.3 Destruction

These examples are probably less interesting than the previous few because the reduction does not make the problem much different. Often the destructive form of CRT just consists of appending the line "By the Chinese Remainder Theorem, it suffices to consider prime powers" and some appropriate embellishments at the end of the solution.

Here is a silly example. There are nicer examples in the practice problems.

Example 3.4 (Math Prize Olympiad 2010)

Prove that for every positive integer n, there exists integers a and b such that $4a^2 + 9b^2 - 1$ is divisible by n.

Proof. It suffices to find such an a and b modulo any prime power.

For 2^k, take $a \equiv 0 \pmod{2^k}$ and $b \equiv 3^{-1} \pmod{2^k}$.

For any other p^k, take $a \equiv 2^{-1} \pmod{p^k}$ and $b \equiv 0 \pmod{p^k}$. □

§4 Practice Problems

Problem 4.1 (IMO 1989)**.** Prove that for every positive integer n, there exists n consecutive positive integers such that none of them is a power of a prime.

Problem 4.2. Let n be a positive integer. Determine, in terms of n, the number of $x \in \{1, 2, \dots, n\}$ for which $x^2 \equiv x \pmod{n}$.

Problem 4.3 (IMO 2009/1)**.** Let n be a positive integer and let $a_1, a_2, a_3, \dots, a_k$ (here $k \geq 2$) be distinct integers in the set $\{1, 2, \dots, n\}$ such that n divides $a_i(a_{i+1} - 1)$ for $i = 1, 2, \dots, k-1$. Prove that n does not divide $a_k(a_1 - 1)$.

Problem 4.4 (APMO 2009/4)**.** Prove that for any positive integer k, there exists an arithmetic progression

$$\frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \dots, \quad \frac{a_k}{b_k}$$

of rational numbers, where a_i, b_i are relatively prime positive integers for each $i = 1, 2, \dots, k$, and moreover the $2k$ numbers a_1, …, a_k, b_1, …, b_k are pairwise distinct.

Problem 4.5 (ELMO Shortlist, Evan Chen)**.** Find all triples (a, b, c) of positive integers such that if n is a positive integer not divisible by any prime less than 2014, then $n + c$ divides $a^n + b^n + n$.

Problem 4.6. Let $a > b > c \geq 3$ be integers. Given that $a \mid bc + b + c$, $b \mid ca + c + a$ and $c \mid ab + a + b$, prove that at least one of a, b, c is not prime.

Problem 4.7 (USA December TST, Iurie Boreico)**.** Prove that for every positive integer n, there exists a set S of n positive integers such that for any two distinct $a, b \in S$, $a - b$ divides a and b but none of the other elements of S.

Problem 4.8 (NIMO, Evan Chen)**.** For a finite set X define

$$S(X) = \sum_{x \in X} x \text{ and } P(x) = \prod_{x \in X} x.$$

Let A and B be two finite sets of positive integers such that $|A| = |B|$, $P(A) = P(B)$ and $S(A) \neq S(B)$. Suppose for any $n \in A \cup B$ and prime p dividing n, we have $p^{36} \mid n$ and $p^{37} \nmid n$. Prove that

$$|S(A) - S(B)| > 5 \cdot 10^7.$$

§5 Challenges

Problem 5.1 (ELMO 2013/5, Andre Arslan)**.** For what polynomials $P(n)$ with integer coefficients can a positive integer be assigned to every lattice point in $\mathbb{R}^3$ so that for every integer $n \geq 1$, the sum of the n^3 integers assigned to any $n \times n \times n$ grid of lattice points is divisible by $P(n)$?

Problem 5.2 (ELMO 2013/3, Victor Wang)**.** Let $m_1, m_2, \dots, m_{2013} > 1$ be 2013 pairwise relatively prime positive integers and $A_1, A_2, \dots, A_{2013}$ be 2013 (possibly empty) sets with $A_i \subseteq \{1, 2, \dots, m_i - 1\}$ for $i = 1, 2, \dots, 2013$. Prove that there is a positive integer N such that

$$N \leq (2|A_1| + 1)(2|A_2| + 1) \cdots (2|A_{2013}| + 1)$$

and for each $i = 1, 2, \dots, 2013$, $N \notin A_i \pmod{m_i}$.

§6 Hints

4.1. Force $p_iq_i \mid x+i$.

4.2. Solve the problem for prime powers dividing n. The answer is a power of two.

4.3. Proceed by contradiction. Look at a prime power $p^r \mid n$, and show that either $a_i \equiv 0 \pmod{p^r}$ $\forall i$ or $a_i \equiv 1 \pmod{p^r}$ $\forall i$.

4.4. Pick x, N such that

$$\frac{x+1}{N}, \dots, \frac{x+k}{N}$$

works after reducing to lowest terms. Force exactly one prime to cancel in each reduction.

4.5. Pick n modulo p and $p-1$ for a large prime p. Force p to divide a constant.

4.6. Simon's Favorite.

4.7. For $n=3$, $x_1\underbrace{}_{2}x_2\underbrace{}_{3}x_3$ gives $\{10,12,15\}$. For $n=4$, $x_1\underbrace{}_{60}x_2\underbrace{}_{90}x_3\underbrace{}_{7}x_4$.

4.8. Show it's divisible by $2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$.

5.1. Look at the one-dimensional case first; the answer is the same.

5.2. Pick t_i for which $t_i \equiv 1 \pmod{m_i}$ and $t_i \equiv 0 \pmod{m_j}$ for $i \neq j$. Look at numbers of the form

$$\sum b_i t_i$$

where $b_i \in B_i$, and B_i is selected so that for any $x, y \in B_i$ we have $x - y \notin A_i$. Show greedily that we can have

$$|B_i| \geq \frac{m_i}{2\,|A_i| + 1}.$$