Chinese Remainder Theorem

EGMO Training Camp 2024

Atonu Roy Chowdhury
atonuroychowdhury@gmail.com

March 2024

When I was a kid, maybe in 3rd or 4th grade, our math textbook had problems like this:

> Find the smallest number that leaves a remainder of 2 when divided by 3, 3 when divided by 4, 4 when divided by 5, 5 when divided by 6, and 6 when divided by 7?

In this case, you see that all the remainders are 1 less than the divisor. So the trick to solve this problem is to take the LCM of all the divisors, and subtracting 1 from that. The LCM of 3, 4, 5, 7 is their product 420. So the answer is 419.

One thing has always baffled me about these problems as a kid. We were told to find the smallest such number. Are there more of such numbers? If so, how can we find all the numbers? Also, how do we know for a fact that such a number always exists? What baffled me more is that everyone else used to think that the existence of such numbers is obvious. Later I've come to know the Chinese remainder theorem, and my childhood query got answered!

§1 Statement

Theorem 1.1 (Chinese Remainder Theorem)
Let $m_1, \ldots, m_k$ be pairwise relatively prime positive integers, and let

$$M = m_1 \cdots m_k.$$

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

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

Proof. The statement can be rewritten as follows: the map

$$F : \mathbb{Z}/M\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

defined by

$$x \bmod M \mapsto (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k) \tag{1}$$

is a bijection. Since the domain and codomain are finite sets with the same cardinality, it suffices to show that F is injective. Suppose $F(x) = F(y)$. Then $x \equiv y \pmod{m_i}$ for each i. So each m_i divides $x - y$. Since all the m_i's are pairwise coprime, their product M also divides $x - y$. So $x \equiv y \pmod{M}$ and hence, F is injective. □

Note that the above proof is non-constructive. It doesn't give us any idea about how to construct $x \bmod M$ given $x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k$. There's a constructive proof as well, but we don't really need the construction for most purposes. Existence and uniqueness is enough for us.

Here's a meme I made a couple years ago when I first learned about infinite dimensional vector spaces and the proof of the existence of their bases using axiom of choice:

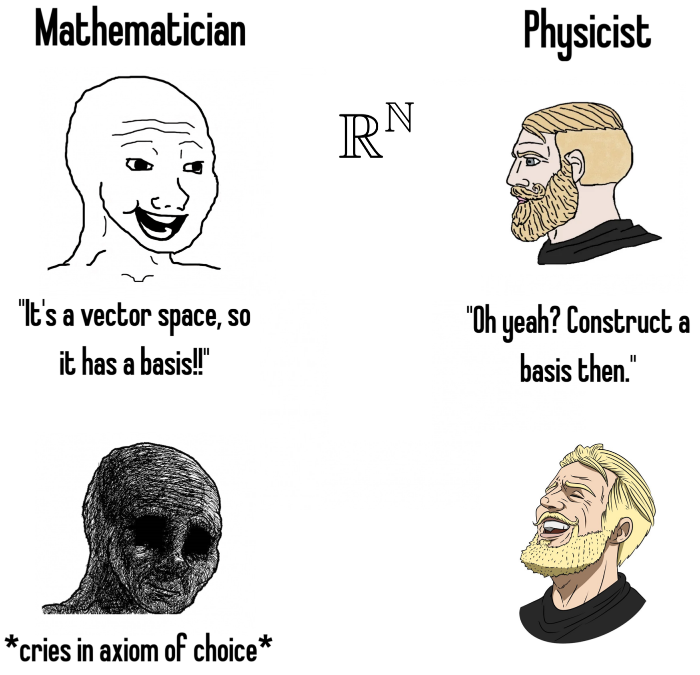
Mathematician
Physicist
$\mathbb{R}^{\mathbb{N}}$
"It's a vector space, so it has a basis!!"
"Oh yeah? Construct a basis then."
cries in axiom of choice

Figure 1: You can ignore the meme if you're unfamiliar with vector spaces or axiom of choice.

There are several useful formulations of CRT. I shamelessly copied the names from Evan Chen's note.

Chinese Remainder Theorem A (Construction)

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

$$x \equiv x_i \pmod{m_i} \tag{2}$$

for each i. Furthermore, this x is unique modulo $M = \prod m_i$.

This perspective is the most useful one for problem solving. It allows us to cook up numbers with desired residues upon division by some numbers. But note that even if m_i's are small, the product M can be very large. As a result, x also can be very large. Furthermore, there is no easy way to write down x in terms of x_i's and m_i's. For the curious minds, suppose $y_i = \frac{M}{m_i}$, and $z_i = y_i^{-1} \bmod m_i$. Then

$$x = \sum_{i=1}^{k} x_i y_i z_i = x_1 y_1 z_1 + x_2 y_2 z_2 + \cdots + x_k y_k z_k \bmod M.$$

To quote Evan Chen,

> "This perspective talks about things we can't actually see."

As I mentioned earlier, we can put together a bunch of (of course, has to be finitely many) linear congruences $x \equiv x_i \pmod{m_i}$, and by CRT, there exists a unique solution $\bmod M$. This notion of CRT goes best with Dirichlet's theorem. In fact, I'd like to call CRT and Dirichlet's theorem *best friends*. Let's see how these two fit together.

Theorem 1.2 (Dirichlet's Theorem)
For any two positive coprime integers a and d, there are infinitely many primes of the form $a + nd$, where n is also a positive integer. In other words, given an arithmetic sequence

$$a_n = a_0 + nd,$$

with $\gcd(a_0, d) = 1$, there are infinitely many n such that a_n is a prime.

According to CRT, since $x \bmod M$ is unique, all the numbers x with the property that

$$x \equiv x_i \pmod{m_i}$$

for each i, are in an arithmetic sequence. A general term of this arithmetic sequence looks like

$$x + Mn, \tag{3}$$

where $n \in \mathbb{Z}$ and x is any number satisfying $x \equiv x_i \pmod{m_i}$ for each i. If, furthermore, we can ensure that x and M are coprime, then we know by Dirichlet's Theorem that there are infinitely many prime numbers in this arithmetic sequence (3). So we can take a prime number P such that $P \equiv x_i \pmod{m_i}$ for each i. Moreover, since there are infinitely many such primes, we can take a sufficiently large prime number with our desired property. This is often useful for sizing and bounding arguments as we shall soon see.

The key point here is, of course, that x and M need to be coprime. There is a really neat way to check it. Since $M = m_1 m_2 \cdots m_k$ and the m_i's are pairwise coprime, we have

$$\gcd(x, M) = \gcd(x, m_1) \gcd(x, m_2) \cdots \gcd(x, m_k). \tag{4}$$

Since $x \equiv x_i \pmod{m_i}$, we have $\gcd(x, m_i) = \gcd(x_i, m_i)$. Therefore,

$$\gcd(x, M) = \gcd(x_1, m_1) \gcd(x_2, m_2) \cdots \gcd(x_k, m_k) = \prod_{i=1}^{k} \gcd(x_i, m_i). \tag{5}$$

If x_i and m_i are coprime for each i, then we can conclude that x and M are coprime. You always have to verify this before applying CRT and Dirichlet's Theorem together.

Chinese Remainder Theorem B (Lifting)

If $x \equiv k \pmod{m_i}$ for each i, then $x \equiv k \pmod{M}$.

This probably does not look very interesting. But this is particularly useful for bounding problems.

Chinese Remainder Theorem C (Destruction)

To understand $x \bmod M$, it suffices to understand $x \bmod m_i$ for every i.

In particular, we can reduce any statement modulo $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ to a statement modulo each $p_i^{\alpha_i}$. If we have perfect information in modulo $p_i^{\alpha_i}$ for each i, CRT allows us to get perfect information in modulo $n = \prod p_i^{\alpha_i}$. This gives us a way to reduce a problem.

§2 Some Examples

Again, quoting Evan Chen:

> "The Chinese Remainder Theorem is a natural, intuitive concept, and therefore it is used most effectively when we don't think explicitly about having to use it."

Let us see some examples where CRT is used. As always, it is recommended that you try the problems on your own for some time before seeing solution ideas.

Example 2.1 (a) Do there exist 14 consecutive positive integers such that each of them is divisible by one or more prime numbers $2 \le p \le 11$?

(b) Do there exist 21 consecutive positive integers such that each of them is divisible by one or more prime numbers $2 \le p \le 13$?

Solution. (a) Among the 14 consecutive numbers, 7 are even, so they are divisible by 2, and we don't need to worry about them. Suppose the odd ones are $n, n+2, n+4, n+6, n+8, n+10, n+12$.

Among these 7 numbers, at most 3 of them are divisible by 3; at most 2 of them are divisible by 5; exactly 1 is divisible by 7; at most 1 is divisible by 11. $3+2+1+1=7$, so we need to have the extreme scenario, and no number can be divisible by more than one prime in the interval $2 \le p \le 11$.

Two consecutive odd multiples of 3 are separated by 6, so we must have that $n, n+6, n+12$ are divisible by 3. Two consecutive odd multiples of 5 are separated by 10. So either $5 \mid n, n+10$ or $5 \mid n+2, n+12$. In either case, either n or $n+12$ is divisible by more than one prime in the interval $2 \le p \le 11$. So there does not exist 14 consecutive such numbers.

(b) At most 11 of the 14 consecutive numbers are even, so we don't need to worry about them. Suppose the odd ones are $n, n+2, \ldots, n+18$.

Let us keep track of which number is divisible by which primes in the following table. We would like to fill this table with primes $2 \le p \le 13$.

number	n	$n+2$	$n+4$	$n+6$	$n+8$	$n+10$	$n+12$	$n+14$	$n+16$	$n+18$
prime										

Let us fill this table greedily. At most 4 of these numbers are divisible by 3, and they are in a gap of 6.

number	n	$n+2$	$n+4$	$n+6$	$n+8$	$n+10$	$n+12$	$n+14$	$n+16$	$n+18$
prime	3			3			3			3

Exactly 2 of these numbers are divisible by 5, and they are in a gap of 10. Since we would like to fill this table completely, the most greedy approach would be to find two numbers that are not divisible by 3.

number	n	$n+2$	$n+4$	$n+6$	$n+8$	$n+10$	$n+12$	$n+14$	$n+16$	$n+18$
prime	3		5	3			3	5		3

At most 2 of these numbers are divisible by 7, and they are in a gap of 14. Again, the most greedy approach would be to find two numbers that are not divisible by 3 or 5.

number	n	$n+2$	$n+4$	$n+6$	$n+8$	$n+10$	$n+12$	$n+14$	$n+16$	$n+18$
prime	3	7	5	3			3	5	7	3

Now only two numbers remain. We can assign 11 and 13 to these numbers.

number	n	$n+2$	$n+4$	$n+6$	$n+8$	$n+10$	$n+12$	$n+14$	$n+16$	$n+18$
prime	3	7	5	3	11	13	3	5	7	3

So this is what we want. But does there exist such n? More precisely, does there exist an odd n which is divisible by 3, $n+4$ is divisible by 5, $n+2$ is divisible by 7, $n+8$ is divisible by 11, $n+10$ is divisible by 13? Of course such n exists by CRT! CRT guarantees us that there exists n that satisfies the following congruences:

$$\begin{aligned} n &\equiv 1 \pmod{2}, \\ n &\equiv 0 \pmod{3}, \\ n &\equiv -4 \pmod{5}, \\ n &\equiv -2 \pmod{7}, \\ n &\equiv -8 \pmod{11}, \\ n &\equiv -10 \pmod{13}. \end{aligned}$$

So we are done!

■

If you actually calculate n, then you'd see $n \equiv 9441 \pmod{30030}$. So, the 21 consecutive numbers are $9440, 9441, \ldots, 9460$. We were taking modulo $2, 3, 5, 7, 11, 13$, which are very small numbers. But in the end, the result turned out to be pretty large.

Example 2.2 (IMO 1989)

Show that for every $n > 1$, there exists n consecutive integers such that none of them are prime powers.

Solution. How can we ensure that a number is not a prime power? If it has more than one prime factors. So we have to ensure that each of the consecutive numbers are divisible by two primes

p, q. Suppose the n consecutive numbers are $N+1, N+2, \ldots, N+n$. So we need

$$\begin{aligned} N+1 &\equiv 0 \pmod{p_1 q_1} \\ N+2 &\equiv 0 \pmod{p_2 q_2} \\ &\vdots \\ N+n &\equiv 0 \pmod{p_n q_n}, \end{aligned} \tag{6}$$

where p_i and q_j are all distinct primes. Since $p_i q_i$ and $p_j q_j$ are coprime, by CRT, there exists such N and we are done! ■

Example 2.3

Show that for every $n > 1$, there exists n consecutive integers such that none of them are sum of two squares.

Solution. What do we know about the numbers that are sum of two squares? We know that if p is an odd prime with $p \equiv 1 \pmod 4$, then p can be written as a sum of two squares. It's obvious that primes $p \equiv -1 \pmod 4$ cannot be written as a sum of two squares, because if $p = x^2 + y^2$, taking mod 4, we get $p \equiv 0, 1, 2 \pmod 4$ since the quadratic residues modulo 4 are $0, 1$.

Also, if A and B are sum of two squares, then so is AB, because of the Brahmagupta-Fibonacci identity:

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = (ac+bd)^2 + (ad-bc)^2. \tag{7}$$

So, if a number only has prime factors of the form $4k+1$, then it can be written as a sum of two squares. What if the number has prime factors $p \equiv -1 \pmod 4$? Suppose $p \mid a^2 + b^2$, where $p \equiv -1 \pmod 4$ is a prime. Then p must divide both a and b. Indeed, if p does not divide a, then suppose a' is the inverse of a modulo p.

$$0 \equiv \left(a^2+b^2\right)\left(a'\right)^2 \equiv \left(aa'\right)^2 + \left(a'b\right)^2 \equiv \left(a'b\right)^2 + 1 \pmod p \tag{8}$$

So -1 is a quadratic residue modulo p. But since $p \equiv -1 \pmod 4$, -1 cannot be a quadratic residue. So we get a contradiction. As a result, p divides a. Similarly, p divides b as well. As a result, $p^2 \mid a^2 + b^2$.

So we have shown that if $p \mid a^2 + b^2$, then $p^2 \mid a^2 + b^2$ for a prime $p \equiv -1 \pmod 4$. Now consider the number

$$\frac{a^2}{p^2} + \frac{b^2}{p^2}. \tag{9}$$

If this sum of squares is divisible by p, then it must be divisible by p^2. In that case, we can reduce the number further by dividing it with p^2. Eventually, we will find that

$$\frac{a^2}{p^{2k}} + \frac{b^2}{p^{2k}} \tag{10}$$

is not divisible by p anymore, for some k. Therefore, the power of p in the prime factorization of $a^2 + b^2$ is even, i.e. $2 \mid v_p\left(a^2+b^2\right)$.

So, if we want to ensure that a number N is not a sum of two squares, it suffices that there is a prime $p \equiv -1 \pmod 4$ such that $v_p(N)$ is odd. How can we ensure that? $N \equiv 0 \pmod{p^{2k-1}}$ does not work. What works is this: $N \equiv p^{2k-1} \pmod{p^{2k}}$. Or simply, $N \equiv p \pmod{p^2}$.

We now need to ensure that there exists n consecutive numbers with this property. Suppose the n consecutive numbers are $N+1, N+2, \dots, N+n$. So we need

$$\begin{aligned} N+1 &\equiv p_1 \pmod{p_1^2} \\ N+2 &\equiv p_2 \pmod{p_2^2} \\ &\vdots \\ N+n &\equiv p_n \pmod{p_n^2}, \end{aligned} \tag{11}$$

where $p_1, p_2, \dots, p_n$ are primes of the form $4k-1$. By CRT, there exists such N, and we are done! ■

Note that, here we implicitly used the fact that there are infinitely many primes of the form $4k-1$. If there are only finitely many such primes, you cannot choose n such primes for **any** n. You can either use Dirichlet's Theorem to convince yourself that there are infinitely many primes of the form $4k-1$. Or you can mimic Euclid's proof of infinitude of primes. If there are only finitely many such primes, say $p_1, \dots, p_m$, then you can take the number

$$4p_1p_2\cdots p_m - 1. \tag{12}$$

It has a prime factor of the form $4k-1$, but none of the p_i's divide it.

Example 2.4 (USAMO 2008)

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 $k_0k_1\dots k_n - 1$ is the product of two consecutive integers.

Solution. If $k_0k_1\dots k_n - 1$ is the product of two consecutive integers, it looks like $m(m+1)$ for some m. So we have

$$m^2+m+1 = k_0k_1\dots k_n. \tag{13}$$

In other words, m^2+m+1 can be written as a product of $n+1$ pairwise coprime numbers. Let's forget about the structure m^2+m+1 for a moment. Given a positive integer N, suppose you want to write N as a product of k pairwise coprime numbers which are all greater than 1. What is the maximum possible value of k? If you think about it a bit, you'll get that the highest possible value of k is the number of distinct prime factors of N. If you express

$$N = n_1n_2\cdots n_k, \tag{14}$$

where the n_i's are pairwise coprime numbers, each n_i contains at least one prime factor of N since they are greater than 1. So k cannot be more than the number of distinct prime factors of N. And this is achievable, since we can just put $n_i = p_i^{\alpha_i}$, for $N = \prod p_i^{\alpha_i}$.

So the question essentially boils down to proving that given $n > 1$, there exists m such that m^2+m+1 has at least $n+1$ distinct prime factors. In other words, numbers of the form m^2+m+1 can have arbitrarily many prime factors.

One consequence of this is that there are infinitely many prime numbers that divide some number of the form m^2+m+1. So it is necessary that we have this. But is it sufficient? Once we have that there are infinitely many primes p such that $p \mid m^2+m+1$, how do we go about proving our original problem? In particular, if

$$\begin{aligned} p_1 &\mid m_1^2+m_1+1, \\ p_2 &\mid m_2^2+m_2+1, \\ &\vdots \\ p_k &\mid m_k^2+m_k+1, \end{aligned}$$

how do we cook up M such that $p_1p_2\cdots p_k \mid M^2+M+1$?

The key trick is that $a-b \mid P(a)-P(b)$ for any integer polynomial P. As a result, if $a \equiv b \pmod{m}$ then $P(a) \equiv P(b) \pmod{m}$. Suppose $P(x)=x^2+x+1$. We have $p_i \mid P(m_i)$. We want to show that there is an "universal" M such that $p_i \mid P(M)$ for each i. So it suffices that we have $M \equiv m_i \pmod{p_i}$ for each i. That way, we would have

$$P(M) \equiv P(m_i) \equiv 0 \pmod{p_i}. \tag{15}$$

Now, by CRT, there exists such M satisfying each of the congruences

$$\begin{aligned} M &\equiv m_1 \pmod{p_1} \\ M &\equiv m_2 \pmod{p_2} \\ &\vdots \\ M &\equiv m_k \pmod{p_k}. \end{aligned} \tag{16}$$

So CRT reduced our problem to proving that there are infinitely many prime numbers that divide some number of the form m^2+m+1. It can be proved by just mimicing Euclid's proof of infinitude of primes. Suppose there are only finitely many primes that divide some number of the form m^2+m+1, say $p_1, p_2, \ldots, p_k$. Then choose $N = p_1p_2\cdots p_k$, and take N^2+N+1. Neither p_i's divide N^2+N+1, so it has a new prime factor, and we are done! ■

There is also another way to finish this problem. A prime p divides some number of the form m^2+m+1 means that the quadratic $x^2+x+1=0$ has a solution in mod p. The solution is

$$x = \frac{-1 \pm \sqrt{-3}}{2}, \tag{17}$$

which is a valid solution mod p if and only if -3 is a quadratic residue modulo p. Let us now use quadratic reciprocity![1]

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right). \tag{18}$$

[1] Check out the first four lines of this: https://www.youtube.com/watch?v=93Bab7S3hjA

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, and

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}. \tag{19}$$

So we have

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right). \tag{20}$$

p is a quadratic residue modulo 3 if and only if $p = 3$ or $p \equiv 1 \pmod 3$. So p divides some number of the form $m^2 + m + 1$ if and only if $p = 3$ or $p \equiv 1 \pmod 3$. There are infinitely many primes $p \equiv 1 \pmod 3$, by Dirichlet's Theorem.

Also, we have proved that there are infinitely many prime numbers that divide some number of the form $m^2 + m + 1$. There is a generalization of this result. It's known as Schur's theorem[2].

Theorem 2.5 (Schur's Theorem)

Suppose P is a polynomial with integer coefficients. Then there exists infinitely many prime numbers p such that $p \mid P(n)$ for some $n \in \mathbb{Z}_{\geq 0}$.

I'm not going to prove it here. You can just mimic Euclid's proof of infinitude of primes (the way we did it for $P(x) = x^2 + x + 1$ in the previous example).

Example 2.6 (APMO 2009)

Prove that for any positive integer k, there exists an arithmetic sequence

$$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \ldots, \frac{a_k}{b_k}$$

of rational numbers, where a_i, b_i are relatively prime positive integers for each $i = 1, 2, \ldots, k$ such that the positive integers $a_1, b_1, a_2, b_2, \ldots, a_k, b_k$ are all distinct.

Solution. An arithmetic sequence of rational number doesn't look very nice when expressed in least form (i.e. when denominator and numerator are coprime). So what we will do is, we are going to consider a common denominator of the rational numbers, then the numerators form an arithmetic progression of integers:

$$\frac{x+d}{N}, \frac{x+2d}{N}, \frac{x+3d}{N}, \ldots, \frac{x+kd}{N}. \tag{21}$$

(We have written the first term to be $x + d$ instead of just x for merely aesthetic reasons. Otherwise, the last term would've been $x + (k-1)d$, which doesn't really look nice.) We need to ensure that when expressed in least terms, the denominators and numerators are all distinct.

When expressed in least terms, the denominators will all look like N/n for some divisor n of N (at first I wrote $\frac{N}{d}$, but later realized that we used d for the common difference of the arithmetic sequence); and when that happens, the numerator is also divisible by that n. Not only that, the gcd of the denominator and N is also exactly n.

[2] There are actually a bunch of results that are known as Schur's theorem. See here: https://en.wikipedia.org/wiki/Schur's_theorem. Also check this out: https://en.wikipedia.org/wiki/List_of_things_named_after_Issai_Schur.

For the denominators to be distinct, the n's have to be distinct for each terms. Therefore, we need N to have at least k different factors $n_1, n_2, \dots, n_k$ such that

$$\begin{aligned} n_1 &\mid x+d, \\ n_2 &\mid x+2d, \\ &\dots \\ n_k &\mid x+kd. \end{aligned} \tag{22}$$

If we want to cook up x with these properties, we need to apply CRT. For that purpose, we need to have n_i's pairwise coprime. The simplest way to make sure of that is choosing each n_i to be a prime p_i. Then

$$N = \prod_{i=1}^{k} p_i = p_1 p_2 \cdots p_k. \tag{23}$$

Since the choice of d also doesn't really matter, we can just choose $d = 1$. Now we have all the ingredients to apply CRT. By CRT, there exists x such that

$$\begin{aligned} x &\equiv -1 \pmod{p_1} \\ x &\equiv -2 \pmod{p_2} \\ &\dots \\ x &\equiv -k \pmod{p_k}. \end{aligned} \tag{24}$$

Then each p_i divides $x + i$. Now we need to ensure that $\gcd(x + i, N) = p_i$. For that purpose, we need to have that for $i \neq j$, p_j does not divide $x + i$. Suppose $p_j \mid x + i$. Since $p_j \mid x + j$, then we have $p_j \mid i - j$. We can solve this issue by taking $p_j > k$, since $|i - j| < k$.

Now we have that $a_i = \frac{x+i}{p_i}$ and $b_i = \frac{N}{p_i}$. Each b_i is distinct. Let's show that a_i and b_j are distinct. Assume otherwise. Then

$$\frac{x+i}{p_i} = a_i = b_j = p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_k. \tag{25}$$

For $k \geq 3$, $\frac{x+i}{p_i}$ is divisible by somoe p_l for $l \neq i$. In other words, $p_l \mid x + i$. Contradiction! (The $k \leq 2$ case is not worth considering, because a sequence is always arithmetic if it has 1 or 2 terms)

Now we just need to prove that a_i's are distinct. $a_i = \frac{x+i}{p_i}$. $x + i$ are strictly increasing, so if we just choose p_i to be strictly decreasing, then we would have that a_i is a strictly increasing sequence. This would ensure that a_i's are distinct. ■

If I had written the solution as you would write on a contest, then the first line would've been like this:

> Consider primes $p_1 > p_2 > p_3 > \cdots > p_k > k$.

You would have zero idea so as to why we need the primes to be greater than k, or why we need the primes to be in decreasing order. Unfortunately, most solutions we see on internet are written like this, without explaining the intuitions. That is why it is extremely important to understand the intuitions while reading solutions.

Example 2.7

Find all functions $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ such that for any $m, n \in \mathbb{Z}_{>0}$,

$$m^n + n^m \mid f(m)^{\varphi(n)} + f(n)^{\varphi(m)}.$$

Solution. Let's just do some random substitutions first (as we do after encountering an FE problem). Let $P\left(m,n\right)$ denote the given assertion. $P(1,1)$ gives $2 \mid 2f\left(1\right)$, which doesn't really give us any new information. From $P(m,m)$, we get

$$m^m \mid f\left(m\right)^{\varphi(m)}.$$

In particular, if p is a prime number,

$$p^p \mid f\left(p\right)^{p-1}. \tag{26}$$

So $f\left(p\right)$ is divisible by p. Not only that, it must be divisible by p^2 as well. Otherwise, if it's divisible by p only and not p^2, then $f\left(p\right)^{p-1}$ is divisible by p^{p-1} only, not p^p.

One thing to notice in this problem is that φ of any random number does not look very nice. The nice outputs of φ are: $\varphi(p) = p-1$ and $\varphi(1) = 1$. So our primary instinct is to substitute primes and 1. So we substitute $m = p$ and $n = 1$ to get

$$p+1 \mid f\left(p\right) + f\left(1\right)^{p-1}. \tag{27}$$

Furthermore, $P(p,q)$ gives us

$$p^q + q^p \mid f\left(p\right)^{q-1} + f\left(q\right)^{p-1}, \tag{28}$$

where p,q are primes. Seemingly, there is nowhere much to go from here. Furthermore, if somehow we get the values of $f(p)$, there is no clear way of finding the values of $f(n)$, for composite n. So we are stuck now. How do we proceed now? One way might be considering prime factors of $p+1$ or p^q+q^p.

Let r be a prime factor of p^q+q^p. Then $r \mid p^q+q^p \mid f\left(p\right)^{q-1} + f\left(q\right)^{p-1}$, i.e.

$$0 \equiv p^q + q^p \equiv f\left(p\right)^{q-1} + f\left(q\right)^{p-1} \pmod{r}. \tag{29}$$

The exponents $p-1$ and $q-1$ are not particularly pretty in mod r, as we have no information about the order of $f\left(p\right)$ or $f\left(q\right)$ modulo r. It would be nice if we had $r-1 \mid p-1$ and $r-1 \mid q-1$. Then we would have

$$0 \equiv f\left(p\right)^{q-1} + f\left(q\right)^{p-1} \equiv 1+1 \equiv 2 \pmod{r},$$

so we could conclude that there is no such f. But it's not necessary that for any prime factor r of p^q+q^p, we would have $r-1 \mid p-1$ and $r-1 \mid q-1$. This is too much to ask to be honest. Also, notice that, in order to produce a contradiction, we don't need it for any prime p,q. Just the mere existence of one pair is sufficient for us. So we need to construct primes p,q,r such that $r \mid p^q+q^p$, $r-1 \mid p-1$, $r-1 \mid q-1$.[3]

Also, once we have $r-1 \mid p-1$, $r-1 \mid q-1$, ensuring $r \mid p^q+q^p$ is not very difficult:

$$p^q + q^p \equiv p \cdot p^{q-1} + q \cdot q^{p-1} \equiv p+q \pmod{r}. \tag{30}$$

So we just need to construct primes p,q,r such that $r-1 \mid p-1$, $r-1 \mid q-1$, $r \mid p+q$. Pick your favorite prime for r (don't choose 57 though). By Dirichlet's Theorem, there is a prime p such that $p \equiv 1 \pmod{r-1}$. Then by CRT and its best friend Dirichlet's Theorem, there is a prime q satisfying

$$\begin{aligned} q &\equiv -p \pmod{r}, \\ q &\equiv 1 \pmod{r-1}. \end{aligned} \tag{31}$$

[3] If you understand Bangla, click here.

So such p, q, r exists, and hence,

$$0 \equiv f(p)^{q-1} + f(q)^{p-1} \equiv 1 + 1 \equiv 2 \pmod{r}. \tag{32}$$

So no such functions exist! Are we done? Well, not really. In (32), we assumed that neither $f(p)$ nor $f(q)$ is divisible by r. Fermat's little theorem states that if p is a prime number **that does not divide** a, then $a^{p-1} \equiv 1 \pmod{p}$. In principle, it's possible that both $f(p)$ and $f(q)$ are divisible by r. And in that case, we don't get any contradiction.

But can we construct p, q, r in such a way that the previous conditions are satisfied, and r does not divide at least one of $f(p)$ and $f(q)$, say $r \nmid f(p)$? Note that we have only used the result of $P(p, q)$. Let us try to use the result of $P(p, 1)$ that we got in (27). Let r be a prime factor of $p + 1$. Then $r \mid p + 1 \mid f(p) + f(1)^{p-1}$, i.e.

$$0 \equiv p + 1 \equiv f(p) + f(1)^{p-1} \pmod{r}. \tag{33}$$

We already have $r - 1 \mid p - 1$, so

$$0 \equiv f(p) + f(1)^{p-1} \equiv f(p) + 1 \pmod{r}. \tag{34}$$

So $r \nmid f(p)$. If you've been paying attention, then you noticed that we have a similar problem here as well. Here also we assumed that $r \nmid f(1)$. But that's not an issue at all. Instead of your favorite prime, we can just choose r to be a prime greater than $f(1)$. After that, we choose the prime p in such a way that

$$\begin{aligned} p &\equiv -1 \pmod{r} \\ p &\equiv 1 \pmod{r-1}. \end{aligned} \tag{35}$$

Again, such a prime exists because of CRT and Dirichlet. As before, we choose q such that

$$\begin{aligned} q &\equiv -p \equiv 1 \pmod{r}, \\ q &\equiv 1 \pmod{r-1}. \end{aligned} \tag{36}$$

Then the corrected version of (32) is

$$0 \equiv f(p)^{q-1} + f(q)^{p-1} \equiv 1 + (\ 0 \text{ or } 1\ ) \equiv 1 \text{ or } 2 \pmod{r}. \tag{37}$$

Thus we get a contradiction, and we are done! ■

I think this example illustrates the importance of being mindful about the edge cases. Even if the theorem is a straightforward and elementary one like Fermat's little theorem, we often tend to overlook the tiny details. Tiny details are not really tiny, as we have seen in this problem.

If you reflect on this problem (and if you clicked on the meme in the last footnote), then you'll understand that we actually treat CRT as our wish-granting genie. Honestly, this is a recurring theme of solving problems using CRT. No matter how many wishes you have, as long as there are finitely many of them and they are compatible (i.e. the m_i's are pairwise coprime), CRT will grant that wish for you.

Example 2.8 (USEMO 2020, easier version)

Prove that for every odd integer $n > 1$, there exist integers $a, b > 0$ such that, if we let $Q(x) = (x+a)^2 + b$, then the following conditions hold:

- we have $\gcd(a,n) = \gcd(b,n) = 1$;
- the number $Q(0)$ is divisible by n; and
- the numbers $Q(1), Q(2), Q(3), \ldots, Q(n)$ each have a prime factor not dividing n.

Solution. We need to show that each $Q(i)$ has a prime factor p_i that does not divide n, for $i = 1, \ldots, n$. That means $p_i \mid (i+a)^2 + b$, i.e. $-b$ is a quadratic residue modulo p_i. The easiest choice for such b is -1, as 1 is a quadratic residue modulo anything. Now we need to see if this works.

For each p_i, a satisfies $(i+a)^2 \equiv 1 \pmod{p_i}$. So we just need that $a + i \equiv 1 \pmod{p_i}$. In order to satisfy $n \mid Q(0)$, we need $n \mid a^2 - 1$, so $a \equiv 1 \pmod{n}$ suffices. Therefore, we can choose $b = -1$ and we can construct a to satisfy

$$\begin{aligned} &a \equiv 1 - i \pmod{p_i} \text{ for each } i = 1, 2, \ldots, n \\ &a \equiv 1 \pmod{n}. \end{aligned} \tag{38}$$

Note that we already have $\gcd(b,n) = 1$, and $a \equiv 1 \pmod{n}$ guarantees that $\gcd(a,n) = 1$. Therefore, we are done. ■

In the original problem, the third condition was

> "the numbers $Q(1), Q(2), Q(3), \ldots$ each have a prime factor not dividing n"

Sure, CRT is our wish-granting machine. But it can only grant finitely many wishes. So just mimicing the above solution does not work for this problem. I will leave this as an exercise for you to work out.

Example 2.9

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

Solution. Since $x^2 \equiv x \pmod{n}$, $n \mid x^2 - x = x(x-1)$. From this we can't conclude either $n \mid x$ or $n \mid x - 1$. We could, if there was only one prime in n. So let us write down the prime power factorization of n:

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}. \tag{39}$$

Then for each i, $p_i^{\alpha_i} \mid x(x-1)$. So either $p_i^{\alpha_i} \mid x$ or $p_i^{\alpha_i} \mid x - 1$. In other words, either $x \equiv 0 \pmod{p_i^{\alpha_i}}$ or $x \equiv 1 \pmod{p_i^{\alpha_i}}$. So, the k-tuple

$$\left(x \bmod p_1^{\alpha_1}, x \bmod p_2^{\alpha_2}, \ldots, x \bmod p_k^{\alpha_k}\right)$$

consists of 0s and 1s only. There are 2^k such possible tuples. By CRT, each of the tuples indicates a unique residue class modulo $\prod p_i^{\alpha_i} = n$. So there are 2^k possible values of x. ■

Example 2.10

Let n be a positive integer and let $a_1, a_2, a_3, \dots, a_k$, $(k \geq 2)$ 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 $a_k(a_1 - 1)$.

Solution. Assume the contrary. Then $n \mid a_i\,(a_{i+1} - 1)$ for all $i = 1, 2, \dots, k$ (here we are taking $a_{k+1} = a_1$). From this, we cannot really deduce that $n \mid a_i$ or $n \mid a_{i+1} - 1$. As much as we want to do it, we can't, because n is not a prime. In these cases, it's often useful to consider the prime powers of n (like Example 2.9).

$$n = \prod_{i=1}^{m} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_m}. \tag{40}$$

Then we have $p^e \mid a_i\,(a_{i+1} - 1)$ for each i (here $p^e \in \{p_1^{\alpha_1}, \dots, p_m^{\alpha_m}\}$). From here as well, as much as we want to write $p^e \mid a_i$ or $p^e \mid a_{i+1} - 1$, we can't. Suppose $p \mid a_i$ for some i. Then

$$p^e \mid a_{i-1}\,(a_i - 1)\,. \tag{41}$$

Since $p \mid a_i$, $p \nmid a_i - 1$. Therefore, $p^e \mid a_{i-1}$. By induction, $p^e \mid a_i$ for each i.

On the other hand, if $p \nmid a_i$, $p^e \mid a_i\,(a_{i+1} - 1)$ gives us that $p^e \mid a_{i+1} - 1$. Then $p \nmid a_{i+1}$. So, by induction, $p^e \mid a_i - 1$ for each i.

Therefore, we see that $a_i \mod p^e$ is a constant sequence, either all 0 or all 1. This holds for all prime p dividing n. Since

$$a_i \bmod p_1^{\alpha_1}, a_i \bmod p_2^{\alpha_2}, \dots, a_i \bmod p_m^{\alpha_m}$$

uniquely determines $a_i \bmod n$, and $a_i \bmod p^e$ is a constant sequence for all p, we can conclude that $a_i \bmod n$ is also a constant sequence. Contradiction! ∎

The following is one of my favorite problems.

Example 2.11 (USA TSTST 2012)

Let $\mathbb{Z}_{>0}$ be the set of positive integers. Let $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ be a function satisfying the following two conditions:

(a) $\gcd(m, n) = 1$ implies $\gcd\left(f\left(m\right), f\left(n\right)\right) = 1$.

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

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

Solution. Attempting a proof by contradiction looks the most natural approach for this problem. Suppose $p \mid f\,(n)$ but $p \nmid n$ for some prime p and positive integer n. We want to produce a contradiction. There is no obvious way of how we can contradict the statement (b) of the problem. So we shall try to contradict (a).

In order to show a contradiction, we need the existence of N such that $\gcd(N, n) = 1$ but $\gcd\left(f(N), f(n)\right) \neq 1$. The only information we have about $f(n)$ is that it is divisible by p. So the only way of showing $\gcd\left(f(N), f(n)\right) \neq 1$ is to show that $p \mid f(N)$.

But then again we encounter another problem. We know nothing about $f(N)$ yet. We just know that N and n are coprime, where $p \nmid n$. So what we can do is, we can try to find N such that $f(N) = N$ and $p \mid N$. Let's take a moment to list the things we want:

(i) $\gcd(N, n) = 1$;

(ii) $p \mid N$;

(iii) $f(N) = N$.

(i) and (ii) are not very hard to get. Since p and n are coprime, we can just take an N that satisfies

$$N \equiv 0 \pmod{p} \text{ and } N \equiv 1 \pmod{n}. \tag{42}$$

The real challence lies in ensuring (iii). We just have a bound that $N \le f(N) \le N + 2012$. In order to show that $f(N) = N$, we need to show that $f(N) = N + i$ are not possible for $i = 1, 2, \ldots, 2012$. Then again, this looks challenging on its own. Since there is no way to contradict (b), we shall again try to contradict (a). For that purpose, we need the existence of M such that $\gcd(M, N) = 1$ but $\gcd(f(M), N + i) \ne 1$ for $i = 1, 2, \ldots, 2012$. That will prove that $f(N) \ne N + i$.

But don't we have the same problem again? We have literally no information about this new variable M we just introduced. So what we have to do is that we have to construct M in such a way that $\gcd(M, N) = 1$ and $\gcd(M + j, N + i) \ne 1$ for $i = 1, 2, \ldots, 2012$ and $j = 0, 1, 2, \ldots, 2012$. Let $p_{i,j}$ is a common prime factor between $M + j$ and $N + i$.

Now we have all the necessary ingredients to solve this problem. Choose 2012×2013 different primes $p_{i,j}$ for $i = 1, 2, \ldots, 2012$ and $j = 0, 1, 2, \ldots, 2012$. Note that the construction of M depends on N, since we must have $\gcd(M, N) = 1$. So we have to construct N first. We construct N such that

$$\begin{aligned} &N \equiv -i \pmod{p_{i,j}} \text{ for } i = 1, 2, \ldots, 2012 \text{ and } j = 0, 1, 2, \ldots, 2012, \\ &N \equiv 0 \pmod{p}, \\ &N \equiv 1 \pmod{n}. \end{aligned} \tag{43}$$

After that we construct M such that

$$\begin{aligned} &M \equiv -j \pmod{p_{i,j}} \text{ for } i = 1, 2, \ldots, 2012 \text{ and } j = 0, 1, 2, \ldots, 2012, \\ &M \equiv 1 \pmod{N}. \end{aligned} \tag{44}$$

We are almost done, we just need to check the compatibility condition. For (43), we need all the $p_{i,j}$'s to be coprime with n and p. This is easily achievable by choosing the primes $p_{i,j}$'s such that $p_{i,j} > \max\{n, p\}$. (44) is a bit more interesting. Here, we need that $p_{i,j}$ and N are coprime. Since $p_{i,j}$ are primes, the only way $p_{i,j}$ and N can fail to be prime is when $p_{i,j} \mid N$. But we already have $p_{i,j} \mid N$. So we just need to ensure that $p_{i,j} \nmid i$. The largest value of i is 2012, so choosing $p_{i,j} > 2012$ suffices. Therefore, the condition on $p_{i,j}$ is

$$p_{i,j} > \max\{2012, n, p\}.$$

After imposing this condition, by CRT, such N and M exists satisfying (43) and (44) and we are done! ■

Example 2.12 (RMM Shortlist 2018)

Determine all polynomials f with integer coefficients such that $f(p)$ is a divisor of $2^p - 2$ for every odd prime p.

Solution. We know that $f(p) \mid 2^p - 2$, and we have no other information. So it's natural that we would like to know more about $f(p)$, for example what are the prime factors of $f(p)$. Clearly, 2 can be a prime factor of $f(p)$, so can p. Because $2 \mid 2^p - 2$ and $p \mid 2^p - 2$. In mod3, 2 is -1. So 2^p is also -1 since p is odd. Therefore, 3 also divides $2^p - 2$. Let us see if there are any more prime factors of $f(p)$.

Let q be a prime (other than $2, 3$ and p) that divides $f(p)$. Then

$$q \mid f(p) \mid 2^p - 2 \implies 2^p \equiv 2 \pmod{q}. \tag{45}$$

We would like to simplify this 2^p term into something manageable, or something we know about. Note that since q is an odd prime, this simplifies to $2^{p-1} \equiv 1 \pmod{q}$. If we can somehow make the exponent something not divisible by $q - 1$, then we would be able to produce a contradiction.

But apparently there's no way to do that directly. So we would take an indirect approach. We can construct a different prime P such that $q \mid f(P)$, so that we have $q \mid 2^{P-1} - 1$, but $P - 1$ is **NOT** divisible by $q - 1$. That way we would be able to show a contradiction. In order to make q divide $f(P)$, we need

$$f(p) \equiv f(P) \pmod{q}. \tag{46}$$

So taking $P \equiv p \pmod{q}$ suffices[4]. Furthermore, we also need that $P - 1$ is **NOT** divisible by $q - 1$. For that purpose, we set $P - 1 \equiv 1 \pmod{q-1}$. Now, by CRT and Dirichlet's Theorem, there are infinitely many prime P satisfying the following congruences:

$$\begin{aligned} P &\equiv p \pmod{q} \\ P - 1 &\equiv 1 \pmod{q-1}. \end{aligned} \tag{47}$$

Well, not quite. Because for implementing Dirichlet along with CRT, in the congruences $x \equiv x_i \pmod{m_i}$, we need that x_i and m_i are coprime. But here, the second congruence is $P \equiv 2 \pmod{q-1}$. 2 and $q - 1$ are not coprime. So we need to tweak it a little bit. We set

$$\begin{aligned} P &\equiv p \pmod{q} \\ P &\equiv -1 \pmod{q-1}. \end{aligned} \tag{48}$$

Then by CRT and Dirichlet's Theorem, there are infinitely many such primes P. We can just take one of them to get

$$\begin{aligned} q \mid f(P) \mid 2^P - 2 &\implies 2^P \equiv 2 \pmod{q} \\ &\implies 2^{-1} \equiv 2 \pmod{q} \\ &\implies 1 \equiv 4 \pmod{q}. \end{aligned} \tag{49}$$

But this is a contradiction to $q \neq 3$. Therefore,

$$f(p) = \pm 2^\alpha 3^\beta p^e. \tag{50}$$

Note that, here α, β, e depends on p, in general. If they were the same for all p, then we could give an argument along the lines of

> $f(x) \mp 2^\alpha 3^\beta x^e$ has infinitely many roots, so it must be the zero polynomial. Therefore, $f(x) = \pm 2^\alpha 3^\beta x^e$.

[4] If $a \equiv b \pmod{m}$ then for any polynomial f of integer coefficients, $f(a) \equiv f(b) \pmod{m}$

But we can't do that here. But we get the idea that perhaps $f(x)$ is of the form cx^n. So we can try to prove that. We can try to factor out the highest power of x that we can.

$$f(x) = x^k g(x). \tag{51}$$

In general, the constant term of f can be 0, but if x^k is the highest power such that we can factor it out, then it forces that the constant term of g has to be nonzero, i.e. $g(0) \neq 0$. Now we want to show that g is a constant polynomial.

We want to show that $g(p)$ takes a constant value for infinitely many primes p. And, we would like to have that $g(p)$ is not divisible by p, so as to have $g(p) = 2^\alpha 3^\beta$. We already have $g(p) \equiv g(0) \pmod{p}$. So in order to make it nonzero, it suffices to take a prime p that doesn't divide $g(0)$. Then $g(p) = \pm 2^\alpha 3^\beta$. Note that, α and β depends on p. If we can find an upper bound for α and β, then we can say that $g(p)$ takes values from a finite set, so there is one value that occurs infinitely often. Then we can conclude that g is a constant polynomial.

One can easily check that $\alpha > 1$ is not possible. Because in that case,

$$4 \mid \pm 2^\alpha 3^\beta = g(p) \mid f(p) \mid 2^p - 2. \tag{52}$$

But $4 \mid 2^p$. Therefore, $\alpha \leq 1$. Similarly, we want to show that $\beta \leq 1$. For $\beta > 1$, we have $9 \mid 2^p - 2$. In other words,

$$2^p \equiv 2^1 \pmod{9}. \tag{53}$$

$\varphi(9) = 6$, and primes can be ± 1 mod 6. Taking p to be 1 mod 6 doesn't produce a contradiction to (53), but -1 mod 6 does. There are infinitely many primes p such that $p \equiv -1 \pmod{6}$ (Dirichlet's Theorem). For those primes,

$$2^p \equiv 2^{-1} \equiv 5 \not\equiv 2 \pmod{9}. \tag{54}$$

Therefore, for those primes, $\beta \leq 1$. So we have,

$$g(p) \in \{\pm 1, \pm 2, \pm 3, \pm 6\} \tag{55}$$

for primes $p \equiv -1 \pmod{6}$. There are infinitely many such primes, so there is one value that occurs infinitely often. Hence, g is a constant polynomial, and the constant value divides 6. Hence,

$$f(x) = cx^k, \tag{56}$$

where $c \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Now, are all the values of k work? Actually, no. For $k \geq 2$, $9 \mid f(3) \mid 2^3 - 2 = 6$ is a contradiction. Therefore,

$$f(x) = \pm 1, \pm 2, \pm 3, \pm 6, \pm x, \pm 2x, \pm 3x, \pm 6x. \tag{57}$$

$f(x) = \pm 3x, \pm 6x$ doesn't work because in that case $9 \mid f(3)$ and we get a contradiction similar to above. It's an easy check that the other solutions work. ■

Example 2.13 (ELMO shortlist 2014)

Find all triples (a, b, c) of positive integers such that if n is not divisible by any prime less than 2014, then $n + c$ divides $a^n + b^n + n$.

Solution. We have that $n + c \mid a^n + b^n - c$. We have to somehow get rid of n here. The idea is: if we can make sure that for an arbitrarily large prime p dividing $n + c$, if we can make it $p \mid a^{\text{constant}} + b^{\text{constant}} - c$, then we can conclude that $a^{\text{constant}} + b^{\text{constant}} - c = 0$. Also we would like to have the constants are small and/or manageable.

Picking a suitable n is the main challenge now. We need to have $p \mid n + c$. Furthermore, for the exponents to be manageable in mod p, we would like to have $n \equiv \pm 1 \pmod{p-1}$. Also, we need to make sure that n is not divisible by primes smaller than 2014. So we set

$$\begin{aligned} n &\equiv -c \pmod{p}, \\ n &\equiv 1 \pmod{p-1}, \\ n &\equiv 1 \pmod{q} \text{ for primes } q < 2014. \end{aligned} \tag{58}$$

There is a small issue with that. $p - 1$ and q are not coprime. For instance, $2 \mid p - 1$. Note that since we have $n \equiv 1 \pmod{p-1}$, then for all "small" primes (by small, I mean less than 2014) q dividing $p - 1$, $n \equiv 1 \pmod{q}$. So we rewrite

$$\begin{aligned} n &\equiv -c \pmod{p}, \\ n &\equiv 1 \pmod{p-1}, \\ n &\equiv 1 \pmod{q} \text{ for primes } q < 2014 \text{ and } q \nmid p-1. \end{aligned} \tag{59}$$

By CRT, such n exists. So we have $p \mid n + c \mid a^n + b^n - c$. In mod p,

$$c \equiv a^n + b^n \equiv a^1 + b^1 \pmod{p}. \tag{60}$$

So $p \mid a + b - c$. This holds for all arbitrarily large prime p. Therefore,

$$a + b = c. \tag{61}$$

In a similar manner, we can set $n \equiv -1 \pmod{p-1}$.

$$\begin{aligned} n &\equiv -c \pmod{p}, \\ n &\equiv -1 \pmod{p-1}, \\ n &\equiv -1 \pmod{q} \text{ for primes } q < 2014 \text{ and } q \nmid p-1. \end{aligned} \tag{62}$$

By CRT, such n exists, and we have

$$c \equiv a^n + b^n \equiv a^{-1} + b^{-1} \pmod{p} \implies abc \equiv a + b \pmod{p}. \tag{63}$$

So $p \mid a + b - abc$. This holds for all arbitrarily large prime p. Therefore,

$$a + b = abc. \tag{64}$$

Equating (61) and (64), we have $c = abc$, so that $ab = 1$. This can only happen when $a = b = 1$. So $(a, b, c) = (1, 1, 2)$. ■

§3 Some Practice Problems

Problem 3.1 (USA TST 2015)**.** Prove that for every $n \in \mathbb{Z}_{>0}$, 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 3.2. A set of positive integers C is called "good" if for all positive integer k, there exists a, b pairwise distinct in C such that $(a + k, b + k) > 1$. Assume that the set C is "good" and the sum of its elements is equal to 2003. Prove that we can eliminate an element c in C such that the remaining elements in C form a "good" set.

Problem 3.3 (ISL 2005)**.** Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$.

Problem 3.4 (USEMO 2020)**.** Prove that for every odd integer $n > 1$, there exist integers $a, b > 0$ such that, if we let $Q(x) = (x + a)^2 + b$, then the following conditions hold:

- we have $\gcd(a, n) = \gcd(b, n) = 1$;
- the number $Q(0)$ is divisible by n; and
- the numbers $Q(1), Q(2), Q(3), \ldots$ each have a prime factor not dividing n.

Problem 3.5 (ELMO 2013)**.** For what polynomials $P(n)$ with integer coefficients can a positive integer be assigned to every lattice point in $\mathbb{Z}^3$ 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 3.6 (ELMO 2013)**.** Let $m_1, m_2, \ldots, m_{2013} > 1$ be 2013 pairwise relatively prime positive integers and $A_1, A_2, \ldots, A_{2013}$ be 2013 (possibly empty) sets with $A_i \subseteq \{1, 2, \ldots, m_i - 1\}$ for $i = 1, 2, \ldots, 2013$. 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 $i = 1, 2, \ldots, 2013$, there does not exist $a \in A_i$ such that m_i divides $N - a$.