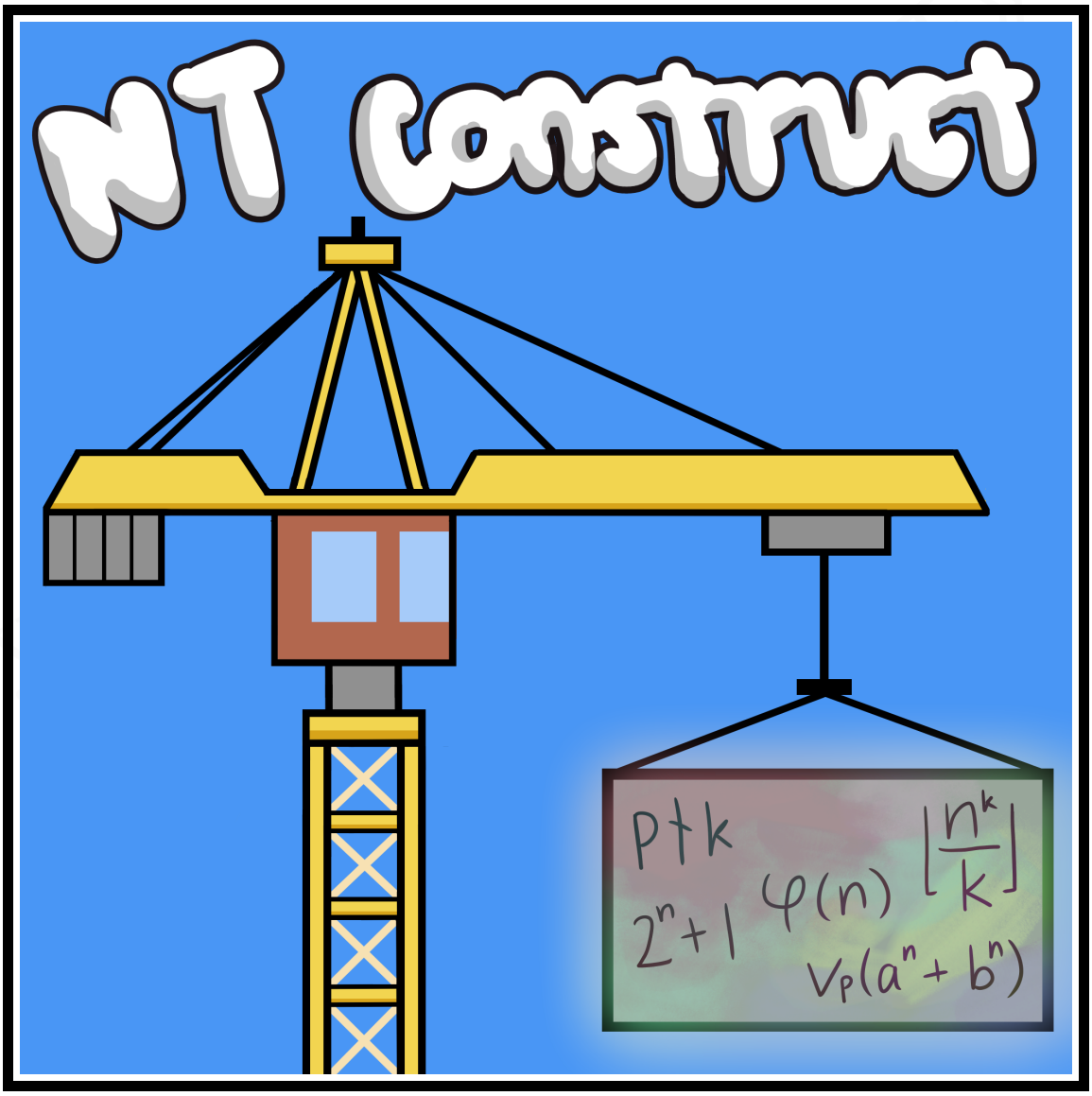
Number Theory Constructions

Evan Chen《陳誼廷》

26 March 2023
DNY-NTCONSTRUCT



OTIS, © Evan Chen, internal use only. Artwork contributed by Heyang Ni.

§1 Lecture Notes

§1.1 Heuristics

This is going to be a lot like the Free class: lots of room for you to make choices (e.g. in constructions). The same two philosophies from the combinatorial counterpart might be helpful here:

- **Experimental**: making conscious design choices, trying things out, etc.
- **Restrictive**: adding abstract constraints, including any constraints you can prove are necessary (which is especially often the case in number theory).

This time, both of these steps often require number theory skill in order to carry out the correct deductions. (So: globally, it feels like doing a combinatorics problem, but locally, it feels like doing a number theory problem.) This has the weird property that sometimes you'd like to rely on statement that is obviously true ("n^2+1 is prime infinitely often"), but either hard to prove or open; if you don't know, then you have to make a judgment call. (Whereas in combinatorics, simple true statements are usually easy to prove.)

Common tropes in this lecture will include:

- Picking really big numbers with lots of prime factors.
- Chinese Remainder Theorem: add modular conditions with reckless abandon, then let CRT collate them for you.
- Appealing to sledgehammers like Bertrand, Dirichlet, Zsigmondy, Kobayashi, et cetera after having reduced the problems to something.

In general, **it's okay to be wasteful!** There are a lot of positive integers. You won't run out.

§1.2 Examples

Example 1.1 (USAMO 2011/4)

Consider the assertion that for each positive integer $n \geq 2$, the remainder upon dividing 2^{2^n} by $2^n - 1$ is a power of 4. Either prove the assertion or find (with proof) a counterexample.

Walkthrough. This is a quick problem showing that you can (and should) often do constructions using both directions: parts (b) and (c) are restrictive, part (d) is experimental.

(a) Show that the problem is equivalent to whether there exists n such that the remainder $2^n \bmod n$ is odd.

(b) Prove that any working n must be odd.

(c) Prove that any working n is composite.

(d) Guess values of n until you find one that works.

In (b) and (c) we were even able to prove n must be odd composite in order to have a chance of working. In other problems you might not be so lucky that you can prove your restrictions are necessary, but it's often correct to take the restriction anyways.

Example 1.2 (TSTST 2015/5)

Let $\varphi(n)$ denote the number of positive integers less than n that are relatively prime to n. Prove that there exists a positive integer m for which the equation $\varphi(n) = m$ has at least 2015 solutions in n.

Walkthrough. There's a couple of ways to approach this problem. The analytic way to go after it is to try and count the number of obtained φ values. Here's a much more concrete approach. Let's start with some informative examples:

(a) Show that $\varphi(3 \cdot 5000) = \varphi(2 \cdot 5000)$.

(b) Show that $\varphi(11 \cdot 1000) = \varphi(10 \cdot 1000)$.

(c) Find another value of n for which $\varphi(n) = \varphi(10000)$.

The idea is that we have a cushion of primes 2*5*. This can work, but we can be much more free with the cushion.

(d) Let $N = 210^{100000000}$. Find some examples of n such that $\varphi(n) = \varphi(N)$, in the spirit of (c).

(e) Construct a set S of 11 prime numbers p for which $p - 1 \mid N$.

(f) Finish the problem.

Example 1.3 (IMO 2003/6)

Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the number $n^p - p$ is not divisible by q.

Walkthrough. In this case it's possible to narrow down the search space right at the beginning.

(a) Show that if $q \not\equiv 1 \pmod{p}$ then this fails. So we will restrict our attention to $q = pk + 1$.

(b) Prove that it's necessary and sufficient to have $p^k \not\equiv 1 \pmod{q}$, for the k in (a).

Okay, so that means for our fixed prime p, we want to find a $q = pk + 1$ such that $q \nmid p^k - 1$. (Funny aside: it would be sufficient that p is a primitive root modulo q, but this is open.)

Dirichlet's theorem at least assures us there are infinitely many $q \equiv 1 \pmod{p}$, but where can we find them? (Aside: something is fishy here; Dirichlet is not an easy theorem to prove, so it is very surprising that a contest is asking us to prove some related result. In fact, even the statement "there exists *any* prime which is $1 \pmod{p}$" is not trivial.)

(c) Suppose $X \not\equiv 1 \pmod{p}$. Prove (if you have not seen it already) that any prime factor q of

$$\Phi(X) = \frac{X^p - 1}{X - 1}$$

is always $1 \pmod{p}$, and in fact $X \pmod{q}$ has order p. (This is called the pth cyclotomic polynomial.)

(d) Prove that if $q \not\equiv 1 \pmod{p^2}$, then $p \nmid k$.

(e) Putting together (c) and (d), pick a suitable value of X and use it to find a way to pick the desired q.

Example 1.4 (USA TST 2015/2)

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.

Walkthrough. The idea is to write

$$S = \{a, a + d_1, a + d_1 + d_2, \ldots, a + d_1 + \cdots + d_{n-1}\}$$

and focus on the difference set first, and only then work on the value of a using an application of Chinese remainder theorem.

(a) Find a set S of the form $S = \{a, a + 2, a + 5\}$. (Here $d_1 = 2$, $d_2 = 3$.)

(b) Characterize all the sets S of the form in (a), i.e. those with $(d_1, d_2) = (2, 3)$.

(c) Show that one can find S of the form $S = \{a, a + 600, a + 1500\}$.

(d) Show that one can find S of the form $S = \{a, a + 600, a + 1500, a + 1507\}$.

(e) Suppose there is a set S of size n with differences $(d_1, \ldots, d_{n-1})$. Prove that we can find an integer M and prime p, such that there is a set S of size $n + 1$ with difference sequence $(Md_1, \ldots, Md_{n-1}, p)$.

(f) Conclude.

By Evan Chen《陳誼廷》, OTIS, Internal Use

§2 Practice Problems

Instructions: Solve [36♣]. If you have time, solve [48♣]. Problems with red weights are mandatory. Try to solve at least one of the two [9♣] problems.

> I'm concerned that we're sitting here like I'm a responsible adult. I'm pretty sure I stopped growing up in my teens and have been faking ever since.
>
> xkcd 616, *Lease*

17AMO1 [2♣] **Problem 1** (USAMO 2017/1)**.** Prove that there exist infinitely many pairs of relatively prime positive integers $a, b > 1$ for which $a + b$ divides $a^b + b^a$.

19USMCA1 [2♣] **Problem 2** (USMCA 2019/1)**.** Kelvin the Frog and Alex the Kat are playing a game on an initially empty blackboard. Kelvin begins by writing a digit. Then, the players alternate inserting a digit anywhere into the number currently on the blackboard, including possibly a leading zero (e.g. 12 can become 123, 142, 512, 012, etc.). Alex wins if the blackboard shows a perfect square at any time, and Kelvin's goal is prevent Alex from winning. Does Alex have a winning strategy?

07SLN2 [2♣] **Problem 3** (Shortlist 2007 N2)**.** Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.

09APMO4 [2♣] **Required Problem 4** (APMO 2009/4)**.** Prove that for any positive integer n, there exists an arithmetic progression

$$\frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \dots, \quad \frac{a_n}{b_n}$$

of rational numbers, such that the $2n$ numbers $a_1, \dots, a_n$ and $b_1, \dots, b_n$ are pairwise distinct, and moreover $\gcd(a_i, b_i) = 1$ for every i.

17SLN2 [2♣] **Problem 5** (Shortlist 2017 N2)**.** Let p be a fixed prime number. Ankan and Ryan play the following turn-based game, with Ankan moving first. On their turn, each player selects an index $i \in \{0, \dots, p-1\}$ not chosen on a previous turn, and a digit $a_i \in \{0, \dots, 9\}$. This continues until all indices have been chosen (hence for p turns). Then, Ankan wins if the number

$$N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_{p-1} 10^{p-1}$$

is divisible by p; otherwise Ryan wins. For each prime p, determine which player has the winning strategy.

19CHN2 [3♣] **Problem 6** (China 2019/2)**.** A *Pythagorean triple* is a set of three distinct positive integers $\{a, b, c\}$ which satisfies $a^2 + b^2 = c^2$. Prove that if P and Q are Pythagorean triples then there exists a finite sequence $P_0, \dots, P_n$ of Pythagorean triples satisfying $P = P_0$, $Q = P_n$, and $P_i \cap P_{i+1} \neq \varnothing$ for each $i = 0, \dots, n-1$.

13SLN3 [3♣] **Problem 7** (Shortlist 2013 N3)**.** Prove that there exist infinitely many positive integers n such that the largest prime divisor of $n^4 + n^2 + 1$ is equal to the largest prime divisor of $(n+1)^4 + (n+1)^2 + 1$.

11BAMO5 [3♣] **Problem 8** (BAMO 2011/5)**.** Decide whether there exists a row of Pascal's triangle containing four pairwise distinct numbers a, b, c, d such that $a = 2b$ and $c = 2d$.

12TSTST5 [3♣] **Problem 9** (TSTST 2012/5)**.** A rational number x is given. Prove that there exists a sequence $x_0, x_1, x_2, \ldots$ of rational numbers with the following properties:

(a) $x_0 = x$;

(b) for every $n \geq 1$, either $x_n = 2x_{n-1}$ or $x_n = 2x_{n-1} + \frac{1}{n}$;

(c) x_n is an integer for some n.

14SLN4 [3♣] **Problem 10** (Shortlist 2014 N4)**.** Let $n > 1$ be an integer. Prove that there are infinitely many integers $k \geq 1$ such that

$$\left\lfloor \frac{n^k}{k} \right\rfloor$$

is odd.

07USATST4 [3♣] **Problem 11** (USA TST 2007/4)**.** Determine whether or not there exist positive integers a and b such that a does not divide $b^n - n$ for all positive integers n.

18CHNTST24 [3♣] **Problem 12** (China TST 2018/2/4)**.** Let k, M be positive integers such that $k-1$ is not squarefree. Prove that there exists a positive real number α such that $\lfloor \alpha \cdot k^n \rfloor$ and M are relatively prime for any positive integer n.

18EGMO2 [3♣] **Problem 13** (EGMO 2018/2)**.** Consider the set

$$A = \left\{ 1 + \frac{1}{k} : k = 1, 2, 3, \ldots \right\}.$$

For every integer $x \geq 2$, let $f(x)$ denote the minimum integer such that x can be written as the product of $f(x)$ elements of A (not necessarily distinct). Prove that there are infinitely many pairs of integers $x \geq 2$ and $y \geq 2$ for which

$$f(xy) < f(x) + f(y).$$

06AMO5 [3♣] **Problem 14** (USAMO 2006/5)**.** A mathematical frog jumps along the number line. The frog starts at 1, and jumps according to the following rule: if the frog is at integer n, then it can jump either to $n+1$ or to $n + 2^{m_n+1}$ where 2^{m_n} is the largest power of 2 that is a factor of n. Show that if $k \geq 2$ is a positive integer and i is a nonnegative integer, then the minimum number of jumps needed to reach $2^i k$ is greater than the minimum number of jumps needed to reach 2^i.

15BRA3 [5♣] **Required Problem 15** (Brazil 2015/3)**.** Given an integer $n > 1$ and its prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, its *false derivative* is defined by

$$f(n) = \alpha_1 p_1^{\alpha_1 - 1} \alpha_2 p_2^{\alpha_2 - 1} \ldots \alpha_k p_k^{\alpha_k - 1}.$$

Prove that there exist infinitely many integers $n > 2$ such that $f(n) = f(n-1) + 1$.

12RMM4 [3♣] **Problem 16** (RMM 2012/4)**.** Prove there are infinitely many integers n such that n does not divide $2^n + 1$, but divides $2^{2^n+1} + 1$.

04IMO6 [5♣] **Required Problem 17** (IMO 2004/6)**.** We call a positive integer *alternating* if every two consecutive digits in its decimal representation are of different parity. Find all positive integers n which have an alternating multiple.

21RMM2

[5♣] **Problem 18** (RMM 2021/2)**.** Xenia and Sergey play the following game. Xenia thinks of a positive integer N not exceeding 5000. Then she fixes 20 distinct positive integers a_1, a_2, ..., a_{20} such that, for each $k = 1, 2, \cdots, 20$, the numbers N and a_k are congruent modulo k. By a move, Sergey tells Xenia a set S of positive integers not exceeding 20, and she tells him back the set $\{a_k : k \in S\}$ without spelling out which number corresponds to which index. How many moves does Sergey need to determine for sure the number Xenia thought of?

12AMO3

[9♣] **Problem 19** (USAMO 2012/3)**.** Determine which integers $n > 1$ have the property that there exists an infinite sequence a_1, a_2, a_3, ...of nonzero integers such that the equality

$$a_k + 2a_{2k} + \cdots + na_{nk} = 0$$

holds for every positive integer k.

16TSTST3

[9♣] **Problem 20** (TSTST 2016/3)**.** Decide whether or not there exists a nonconstant polynomial $Q(x)$ with integer coefficients with the following property: for every positive integer $n > 2$, the numbers

$$Q(0),\ Q(1), Q(2),\ \ldots,\ Q(n-1)$$

produce at most $0.499n$ distinct residues when taken modulo n.

13SLN4

[5♣] **Required Problem 21** (Shortlist 2013 N4)**.** Determine whether there exists an infinite sequence of nonzero digits a_0, a_1, a_2, a_3, ...such that the number $\overline{a_k a_{k-1} \ldots a_1 a_0}$ is a perfect square for all sufficiently large k.

20AUS8

[2♣] **Problem 22** (Australia 2020/8)**.** Prove that for each integer k satisfying $2 \le k \le 100$, there are positive integers b_2, b_3, ..., b_{101} such that

$$b_2^2 + b_3^3 + \cdots + b_k^k = b_{k+1}^{k+1} + b_{k+2}^{k+2} + \cdots + b_{101}^{101}.$$

[1♣] **Mini Survey.** Fill out feedback on the OTIS-WEB portal when submitting this problem set. Any thoughts on problems (e.g. especially nice, instructive, easy, etc.) or overall comments on the unit are welcome.

In addition, if you have any suggestions for problems to add, or want to write hints for one problem you really liked, please do so in the ARCH system!

The maximum number of [♣] for this unit is [81♣], including the mini-survey.

By Evan Chen《陳誼廷》
Not for Internal Use

§3 Solutions to the walkthroughs

§3.1 Solution 1.1, USAMO 2011/4

We claim $n = 25$ is a counterexample. Since $2^{25} \equiv 2^0 \pmod{2^{25}-1}$, we have

$$2^{2^{25}} \equiv 2^{2^{25} \bmod 25} \equiv 2^7 \bmod 2^{25}-1$$

and the right-hand side is actually the remainder, since $0 < 2^7 < 2^{25}$. But 2^7 is not a power of 4.

> **Remark.** Really, the problem is just equivalent for asking 2^n to have odd remainder when divided by n.

§3.2 Solution 1.2, TSTST 2015/5

Here are two explicit solutions.

¶ First solution with ad-hoc subsets, by Evan Chen I consider the following eleven prime numbers:

$$S = \{11, 13, 17, 19, 29, 31, 37, 41, 43, 61, 71\}.$$

This has the property that for any $p \in S$, all prime factors of $p-1$ are one digit.

Let $N = (210)^{\text{billion}}$, and consider $M = \varphi(N)$. For any subset $T \subset S$, we have

$$M = \varphi\left(\frac{N}{\prod_{p \in T}(p-1)} \prod_{p \in T} p \right).$$

Since $2^{|S|} > 2015$ we're done.

> **Remark.** This solution is motivated by the deep fact that $\varphi(11 \cdot 1000) = \varphi(10 \cdot 1000)$, for example.

¶ Second solution with smallest primes, by Yang Liu Let $2 = p_1 < p_2 < \cdots < p_{2015}$ be the *smallest* 2015 primes. Then the 2015 numbers

$$\begin{aligned} n_1 &= (p_1 - 1)p_2 \dots p_{2015} \\ n_2 &= p_1(p_2 - 1) \dots p_{2015} \\ &\vdots \\ n_{2015} &= p_1 p_2 \dots (p_{2015} - 1) \end{aligned}$$

all have the same phi value, namely

$$\varphi(p_1 p_2 \dots p_{2015}) = \prod_{i=1}^{2015} (p_i - 1).$$

§3.3 Solution 1.3, IMO 2003/6

By orders, we must have $q = pk + 1$ for this to be possible. So we just need $n^p \not\equiv p \iff p^k \not\equiv 1 \pmod q$.

So we need a prime $q \equiv 1 \pmod p$ such that $p^k \not\equiv 1 \pmod q$. To do this, we first recall the following lemma.

Lemma

Let $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$. For any integer a, if q is a prime divisor of $\Phi_p(a)$ other than p, then $a \pmod q$ has order p. (In particular, $q \equiv 1 \pmod p$.)

Proof. We have $a^p - 1 \equiv 0 \pmod q$, so either the order is 1 or p. If it is 1, then $a \equiv 1 \pmod q$, so $q \mid \Phi_p(1) = p$, hence $q = p$. □

Now the idea is to extract a prime factor q from the cyclotomic polynomial

$$\Phi_p(p) = \frac{p^p - 1}{p - 1} \equiv 1 + p \pmod{p^2}$$

such that $q \not\equiv 1 \pmod{p^2}$; hence $k \not\equiv 0 \pmod p$, and as $p \pmod q$ has order p we have $p^k \not\equiv 1 \pmod q$.

§3.4 Solution 1.4, USA TST 2015/2

The idea is to look for a sequence $d_1, \dots, d_{n-1}$ of "differences" such that the following two conditions hold. Let $s_i = d_1 + \cdots + d_{i-1}$, and $t_{i,j} = d_i + \cdots + d_{j-1}$ for $i \le j$.

(i) No two of the $t_{i,j}$ divide each other.

(ii) There exists an integer a satisfying the CRT equivalences

$$a \equiv -s_i \pmod{t_{i,j}} \quad \forall i \le j$$

Then the sequence $a + s_1$, $a + s_2$, …, $a + s_n$ will work. For example, when $n = 3$ we can take $(d_1, d_2) = (2, 3)$ giving

$$10 \underbrace{\overbrace{}^{5}}_{2} 12 \underbrace{}_{3} 15$$

because the only conditions we need satisfy are

$$\begin{aligned} a &\equiv 0 \pmod 2 \\ a &\equiv 0 \pmod 5 \\ a &\equiv -2 \pmod 3. \end{aligned}$$

But with this setup we can just construct the d_i inductively. To go from n to $n+1$, take a $d_1, \dots, d_{n-1}$ and let p be a prime not dividing any of the d_i. Moreover, let M be a multiple of $\prod_{i \le j} t_{i,j}$ coprime to p. Then we claim that $d_1 M, d_2 M, \dots, d_{n-1} M, p$ is such a difference sequence. For example, the previous example extends as follows with $M = 300$ and $p = 7$.

$$a \underbrace{\overbrace{\overbrace{}^{1507}}^{907}}_{600} b \underbrace{}_{900} c \underbrace{}_{7} d$$

The new numbers p, $p+Md_{n-1}$, $p+Md_{n-2}$, ...are all relatively prime to everything else. Hence (i) still holds. To see that (ii) still holds, just note that we can still get a family of solutions for the first n terms, and then the last $(n+1)$st term can be made to work by Chinese Remainder Theorem since all the new $p+Md_k$ are coprime to everything.

By Evan Chen《陳誼廷》
OTIS, Internal Use