Number Theory Constructions

Evan Chen[*]

DNY-NTCONSTRUCT

§1 Lecture Notes

§1.1 Discussion

§1.2 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:

- **Concrete**: making conscious design choices, or narrowing the set of things you're considering.
- **Abstract**: 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 rarely impossible to prove.)

Common tropes in this lecture will include:

- Picking really numbers big 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.

§1.3 Examples

Example 1.1 (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.

[*] Internal use: Olympiad Training for Individual Study (OTIS). Last update May 17, 2018.

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 1.2 (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 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 $q \nmid p^k - 1$. Dirichlet's theorem at least assures us there are infinitely many $q \equiv 1 \pmod{p}$, but where can we find them?

(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 $q \pmod{p}$ has order p. (This is called the pth cyclotomic polynomial.)

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

(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 1.3 (December 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 that is to write $S = \{a, a+d_1, a+d_1+d_2, \dots, a+d_1+\dots+d_{n-1}\}$ 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 $(d_1, \dots, d_{n-1})$ Prove that we can find an integer M and prime p, such that there is a set S of size $n+1$ one with $(Md_1, \dots, Md_{n-1}, p)$

(f) Conclude.

§2 Practice Problems

Solve at least [35♣]. If you are ambitious, aim for [50♣] or more. Problems whose weights are marked in red are mandatory. Try to solve at least one of the three [9♣] problems.

[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 $a^b + b^a$.

[5♣] **Problem 2** (JMO 2016/2). Prove that there exists a positive integer $n < 10^6$ such that 5^n has six consecutive zeros in its decimal representation.

[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.

[2♣] **Problem 4** (IMO 2000/5). Does there exist a positive integer n such that n has exactly 2000 prime divisors and n divides $2^n + 1$?

[3♣] **Problem 5** (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 $c = 2d$.

[3♣] **Problem 6** (TSTST 2012/5). A rational number x is given. Prove that there exists a sequence $x_0, x_1, x_2, \dots$ of rational numbers with the following properties:

(a) $x_0 = x$;

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

(c) x_n is an integer for some n.

[3♣] **Problem 7** (Shortlist 2014 N4). Let $n > 1$ be an integer. Prove that there are infinitely many integers $k \ge 1$ such that

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

is odd.

[3♣] **Problem 8** (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.

[3♣] **Problem 9** (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.

[3♣] **Problem 10** (EGMO 2018/2)**.** Consider the set

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

For every integer $x \ge 2$, 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 $x \ge 2$ and $y \ge 2$ for which

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

[5♣] **Problem 11** (USAMO 2006/3)**.** For integral m, let $p(m)$ be the greatest prime divisor of m. By convention, we set $p(\pm 1) = 1$ and $p(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence

$$\{p(f(n^2)) - 2n\}_{n \ge 0}$$

is bounded above. (In particular, this requires $f(n^2) \neq 0$ for $n \ge 0$.)

[5♣] **Problem 12** (USAMO 2013/5)**.** Let m and n be positive integers. Prove that there exists an integer c such that cm and cn have the same nonzero decimal digits.

[5♣] **Problem 13** (RMM 2012/4)**.** Prove there are infinitely many integers n such that n does not divide $2^n + 1$, but divides $2^{2^n+1} + 1$.

[9♣] **Problem 14** (USAMO 2012/3)**.** Determine which integers $n > 1$ have the property that there exists an infinite sequence a_1, a_2, a_3, $\dots$ of nonzero integers such that the equality

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

holds for every positive integer k.

[9♣] **Problem 15** (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

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

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

[5♣] **Problem 16** (Shortlist 2013 N4)**.** Determine whether there exists an infinite sequence of nonzero digits a_1, a_2, a_3, $\dots$ such that the number $\overline{a_k a_{k-1} \dots a_1}$ is a perfect square for all sufficiently large k.

[5♣] **Problem 17** (EGMO 2014/3)**.** We denote the number of positive divisors of a positive integer m by $d(m)$ and the number of distinct prime divisors of m by $\omega(m)$. Let k be a positive integer. Prove that there exist infinitely many positive integers n such that $\omega(n) = k$ and $d(n)$ does not divide $d(a^2 + b^2)$ for any positive integers a, b satisfying $a + b = n$.

[9♣] **Problem 18** (IMO 2017/6)**.** An *irreducible lattice point* is an ordered pair of integers (x, y) satisfying $\gcd(x, y) = 1$. Prove that if S is a finite set of irreducible lattice points then there exists a *homogeneous* polynomial $f(x, y)$ of degree at least 1 such that $f(x, y) = 1$ for each $(x, y) \in S$.

§3 Solutions to the walkthroughs

§3.1 Solution 1.1, TSTST 2015/5

I consider the following ELEVEN PRIME NUMBERS:

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

It 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 $M = \phi(N)$. For any subset $T \subset S$, we have

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

Since $2^{|T|} > 2015$ we're done.

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

§3.2 Solution 1.2, 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 $p^k \not\equiv 1 \pmod q$. Wishfully we hope the order of p is p and $k \nmid p$. One way to do this is extract a prime factor from the cyclotomic polynomial

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

which does not happen to be $1 \pmod{p^2}$.

§3.3 Solution 1.3, December 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 $s_i = d_1 + \dots + d_{i-1}$, and $t_{i,j} = d_i + \dots + d_{j-1}$ 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 $a + s_1$, $a + s_2$, $\dots$, $a + s_n$ will work. For example, when $n = 3$ we can take $(d_1, d_2) = (2, 3)$ giving

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

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 $M = \prod_{i=1}^{n-1} d_i$.

Then we claim that $d_1M, d_2M, \dots, d_{n-1}M, p$ is such a difference sequence. For example, the previous example extends as follows.

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

The new numbers p, $p+Md_{n-1}$, $p+Md_{n-2}$, $\dots$ 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.