Sledgehammers in number theory

CJ Quines

June 15, 2023

Do you like the feeling of killing flies with bazookas? Have you ever wanted to learn theorems that are useful in olympiad number theory but are too powerful to cite? Are you interested in reading things that can be actively harmful for your competition math career? Then I have the perfect handout for you…

1. Notation

Standard notation I'll use:

- $\mathbb{N}$ is the set of positive integers.
- $\mathbb{Z}[x]$ is the set of polynomials with integer coefficients.
- $\{a_n\}_{n=1}^N$ is $\{a_1, a_2, \dots, a_N\}$. We'll also write $\{a_n\}_{n\geq 1}$ for $\{a_n\}_{n=1}^\infty$.

Less standard notation I'll use:

- $\mathbb{P}$ is the set of primes.
- $\mathbb{P}(S)$, or the **prime divisors** of S, is the set of $p \in \mathbb{P}$ such that there's some $s \in S$ with $s \neq 0$ and $p \mid s$. (Why do we have to say $s \neq 0$?)

Abuses of notation:

- We write $\{a_n\}$ for $\{a_n\}_{n\geq 1}$ because it's so common. For example, the odd positive integers are $\{2n - 1\}$. We'll never write sets with one element, so there should be no risk of confusion.
- We write $\mathbb{P}\{a_n\}$ instead of $\mathbb{P}(\{a_n\})$.

When stating results, I'll rate them with their "citability", which is how fine I'd be citing it in a solution for an oly problem, and "usefulness", which is how applicable I think it is. These are scaled from 1 to 5, where 1 is least and 5 is most, rated based on a completely subjective assessment I totally made up. For example:

> **Theorem. Irrationality of $\sqrt{2}$.** Citability: 5 Usefulness: 1
>
> There are no $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$.

I hope you're fine with treating results as black boxes, because I'll be skipping lots of proofs. Here we go.

2. Hammers

2.1. Chebotarev density theorem

Stating the Chebotarev density theorem in full generality needs Galois theory. There's a bunch of weaker versions of Chebotarev, like the Frobenius or Kronecker density theorems (which also need Galois theory), or the density version of Dirichlet's theorem, which we cover later.

I have this section for two reasons. First, when I later mention Chebotarev, you'll know what I'm referring to. Second is to define the notion of *density* in the first place. If $S \subseteq \mathbb{P}$, then there's *two* notions of S's density. The first is **natural density**:

$$\delta(S) = \lim_{N\to\infty} \frac{|\{p \in S, p \le N\}|}{|\{p \in \mathbb{P}, p \le N\}|},$$

and the second is **Dirichlet density**:

$$\delta'(S) = \lim_{s\to 1^+} \frac{\sum_{p\in S} \frac{1}{p^s}}{\sum_{p\in\mathbb{P}} \frac{1}{p^s}}.$$

Dirichlet density looks weird, but it's easier to work with analytically, which is why most results below actually use Dirichlet density. There's a result that says that if $\delta(S)$ exists, then it is equal to $\delta'(S)$. The converse isn't true, but you probably won't run into the counterexamples in practice. We'll thus be lazy and conflate the two notions of density; if you're making a density argument it doesn't matter anyway.

2.2. Schur-type results

Here's something I'll feel no qualms citing in an olympiad:

Theorem. Schur's theorem. Citability: 5 Usefulness: 4

If $f \in \mathbb{Z}[x]$ is nonconstant, then $\mathbb{P}\{f(n)\}$ is infinite.

There are many proofs of this. I'll cite a result of Elsholtz in [Els12], which is stronger than Schur and has an elementary counting proof:

Theorem. Schur's theorem (growth). Citability: 1 Usefulness: 1

Suppose that $\{a_n\}$ has:

- subexponential growth: for all $\varepsilon > 0$, we have $a_n \le 2^{n^\varepsilon}$ as $n \to \infty$, and
- almost-injectivity: there's some c such that each integer appears in $\{a_n\}$ at most c times.

Then $\mathbb{P}\{a_n\}$ is infinite.

Proof. We prove a special case, assuming $a_n > 0$ and that it's almost-injective with $c = 1$. These conditions means that $a_1, \ldots, a_n$ have n distinct values. Suppose $\mathbb{P}\{a_n\} = \{p_1, \ldots, p_k\}$. The main idea is to count possible prime factorizations, and show it's too few compared to the n we need. If we factorize a_n as $\prod p_i^{e_i}$, we must have $e_i < n^\varepsilon$ due to subexponential growth. That means that there's at most $(n^\varepsilon)^k$ prime factorizations, which for large n, is too few. □

The growth version covers, for example, $\{\lfloor \pi n^2 \rfloor\}$, which Schur alone doesn't. This combinatorial proof is similar to Erdős's proof there are infinitely many primes, which I recount in [Qui19].

We can also strengthen Schur to specify the density, as a corollary of Chebotarev:

Theorem. Schur's theorem (density). Citability: 1 Usefulness: 3

If $f \in \mathbb{Z}[x]$ is nonconstant, then $\mathbb{P}\{f(n)\}$ has density at least $\frac{1}{\deg f}$.

If you want a reference, check the upper bound in Lemma 3 of [BL06].

2.3. Anti-Schur-type results

If $f \in \mathbb{Z}[x]$, then saying that $p \in \mathbb{P}\{f(n)\}$ is the same as saying that $f(x) \equiv 0 \pmod{p}$ has a solution, or in other words, it has a root modulo p. Thus, Schur can be restated as "a nonconstant polynomial has roots modulo infinitely many primes."

Can we say things about primes that f *doesn't* have roots in, or the set $\mathbb{P} \setminus \mathbb{P}\{f(n)\}$? We should rule out the case where f has a linear factor (in $\mathbb{Q}$): for example, $6x - 1$ has a root modulo every prime except 2 and 3. The tentative claim is then: a polynomial without linear factors has no roots modulo infinitely many primes.

Unfortunately, this isn't true. A counterexample is $(x^2-2)(x^2-3)(x^2-6)$, because modulo any prime, at least one of 2, 3, and 6 is a quadratic residue. So "without linear factors" is too weak of an assumption. The correct result requires an **irreducible** polynomial, one that can't be factored as the product of two nonconstant polynomials:

Theorem. Anti-Schur's theorem. Citability: 1 Usefulness: 1

If $f \in \mathbb{Z}[x]$ is irreducible with $\deg f \geq 2$, then $\mathbb{P} \setminus \mathbb{P}\{f(n)\}$ is infinite.

Another way to say this is that if $f \in \mathbb{Z}[x]$ has roots modulo every prime, then it's either reducible or linear. The previously cited Lemma 3 of [BL06] gives a density version of anti-Schur in its lower bound:

Theorem. Anti-Schur's theorem (density). Citability: 1 Usefulness: 1

If $f \in \mathbb{Z}[x]$ is irreducible with $\deg f \geq 2$, then $\mathbb{P} \setminus \mathbb{P}\{f(n)\}$ has density at least $\frac{1}{(\deg f)!}$.

As an aside, $x^8 - 16$ is another counterexample to our earlier claim; it factorizes as $(x^2-2)(x^2+2)(x^4+4)$, which for similar reasons also has a root modulo any prime. This also serves as a counterexample to "if something is an nth power modulo every prime, it's an nth power." This statement is *almost* true. The Grunwald–Wang theorem classifies the exceptions, and in the $\mathbb{Q}$ case, we get:

Theorem. Grunwald–Wang theorem (for $\mathbb{Q}$). Citability: 1 Usefulness: 1

Suppose a is an nth power modulo a set of primes with density 1. Then either a is an nth power, or $8 \mid a$ and $a = 2^{n/2} b^n$ for some b.

See the discussion in 9.B of [AD12].

2.4. Kobayashi's theorem

While Schur-type results prove that the prime divisors of many integer sequences are infinite, there's some that it doesn't cover, like $\mathbb{P}\{2^n+1\}$, or $\mathbb{P}\{2^{2^n}+1\}$, or $\mathbb{P}\{\lfloor 10^n\pi\rfloor\}$. I think it's open whether the third set is infinite, but the first two are covered by Kobayashi's theorem:

> **Theorem. Kobayashi's theorem.** Citability: 3 Usefulness: 3
>
> Let $t \in \mathbb{Z}$ be nonzero and $\{a_n\}$ unbounded. If $\mathbb{P}\{a_n\}$ is finite, then $\mathbb{P}\{a_n+t\}$ is infinite.

Kobayashi's original paper [Kob81] is one that's well-known-ish in olympiad circles, but I can only find one other paper that cites it, [Mor90]. I also can't find anything Hiroshi Kobayashi did outside this paper. The affiliation given is "Ebina Highschool", which is not only a *high school*, but one I can't find any records of.

No elementary proof of Kobayashi is known, but somehow it's wormed its way into olympiad canon, which raises its citability by a bit. Kobayashi's original proof uses Siegel's theorem. There's a nice proof by mavropnevma in [Sch11] that uses Thue's theorem, which I'll state in subsection 2.5. mavropnevma's proof is nice enough (and the trick common enough) that I'll reproduce it:

Proof. Write $a_n = ax^3$ and $a_n + t = by^3$ for a and b cubefree.[1] If $\mathbb{P}\{a_n\}$ and $\mathbb{P}\{a_n+t\}$ are finite, there's only finitely many possible a and b, and hence a finite number of equations $by^3 - ax^3 = t$. By Thue, each has a finite number of solutions, contradicting the fact that $\{a_n\}$ is unbounded. □

2.5. Roth's theorem

Let's take a brief digression to talk about Thue, and its generalization Roth's theorem. We call a polynomial **homogeneous** if each term has the same degree, like in x^2+xy+y^2. The set of two-variable degree-d homogeneous polynomials is written $\mathbb{Z}^d[x,y]$. For $k \in \mathbb{Z}$ and $f \in \mathbb{Z}^d[x,y]$, we want to study the Diophantine equation $f(x,y) = k$.

The method for solving these depends on d. When $d = 1$ this is elementary. When $d = 2$ it usually reduces to a generalized Pell equation, see for example [Dju07]. And when $d \geq 3$ we have Thue:

> **Theorem. Thue's theorem.** Citability: 1 Usefulness: 2
>
> Let $d \geq 3$ and $k \in \mathbb{Z}$. If $f \in \mathbb{Z}^d[x,y]$ is irreducible, then $f(x,y) = k$ has finitely many integer solutions.

These days it's proven as a consequence of the stronger Roth's theorem. The idea is that if $f(x,y) = k$, then $f(x/y, 1) = k/y^d$. If y is large, then k/y^d is close to 0, so we'd get that x/y approximates some root α of $f(\alpha, 1) = 0$, and Roth would finish.

To state Roth, we first define an algebraic number. We say that $\alpha \in \mathbb{R}$ is **algebraic** if there's some $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Roth tells us that algebraic numbers can't have many "good" approximations:

[1] A number is cubefree if each exponent of a prime in its prime factorization is at most 2. Alternatively, a number is cubefree if it's not divisible by a perfect cube other than 1.

Theorem. Roth's theorem. Citability: 1 Usefulness: 1

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be algebraic. Then for every $\varepsilon > 0$, there's only finitely many solutions to

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{y^{2+\varepsilon}}$$

with relatively prime x, y.

Roth is a deep theorem from Diophantine geometry, where algebraic geometry methods are used to tackle Diophantine equations; see Appendix A for an overview.

2.6. Zsigmondy sets

Kobayashi shows that $\mathbb{P}\{2^n + 1\}$ is infinite, but we can say more than that. Call p a **primitive prime divisor** of some sequence $\{a_n\}$ if $p \mid a_n$ but $p \nmid a_k$ for every $k < n$. Because $\mathbb{P}\{2^n + 1\}$ is infinite, we expect there to be infinitely many primitive prime divisors as well. Zsigmondy's theorem says that primitive divisors aren't just infinite; almost all terms have them.

Given a sequence $\{a_n\}$, we define its **Zsigmondy set** $\mathcal{Z}\{a_n\}$ as the set of $n \geq 1$ such that a_n *doesn't* have a primitive prime divisor. In other words, $n \in \mathcal{Z}\{a_n\}$ if $p \mid a_n$ implies $p \mid a_k$ for some $k < n$. Then:

Theorem. Zsigmondy's theorem. Citability: 4 Usefulness: 5

If a and b are relatively prime, then $\mathcal{Z}\{a^n - b^n\} \subseteq \{1, 2, 6\}$. In particular:

- $1 \in \mathcal{Z}\{a^n - b^n\}$ iff $a - b = 1$,
- $2 \in \mathcal{Z}\{a^n - b^n\}$ iff $a + b$ is a power of 2, and
- $6 \in \mathcal{Z}\{a^n - b^n\}$ iff $a = 2$ and $b = 1$.

Similarly, $\mathcal{Z}\{a^n + b^n\} = \varnothing$, with the exception of $2^3 + 1^3$.

Zsigmondy is an elementary result; see [Mic14] for a proof. There's other theorems about Zsigmondy sets. The most useful one for olympiads would probably be Carmichael's theorem:

Theorem. Carmichael's theorem. Citability: 2 Usefulness: 1

Let p and q be relatively prime with $p^2 > 4q$ and $pq \neq 0$. Define $\{u_n\}$ by $u_0 = 0$, $u_1 = 1$, and $u_n = pu_{n-1} - qu_{n-2}$. Then $\mathcal{Z}\{u_n\} \subseteq \{1, 2, 6, 12\}$.

The $\{u_n\}$ here is known as a Lucas sequence of the first kind; it's usually written $\{U_n(p, q)\}$. Carmichael is again an elementary result, see [Yab01].

2.7. Bertrand-type results

There's a verse about Bertrand's postulate by NJ Fine which goes "Chebyshev said it, but I'll say it again / There's always a prime between n and $2n$." Actually, what Bertrand conjectured and Chebyshev proved was a mildly stronger version:

Theorem. Bertrand's postulate. Citability: 5 Usefulness: 3

If $n > 3$, then there's some prime p such that $n < p < 2n - 2$.

Although it's not the first proof, it's Erdős's proof of Bertrand that is the most famous, in part because it's elementary. The idea is to show that $\binom{2n}{n}$ must have a prime factor between n and $2n$ due to size; see [Bog18] for an exposition.

A stronger result, in the direction of having a smaller interval, is Sylvester–Schur:

Theorem. Sylvester–Schur theorem. Citability: 4 Usefulness: 1

If $n \geq 2k$, then $\binom{n}{k}$ has a prime divisor greater than k.

The famous proof is Erdős's, [Erd34]. In [Han73], it's shown that it has a prime divisor greater than $\frac{3}{2}k$, with exceptions $\binom{4}{2}$, $\binom{9}{2}$, and $\binom{10}{5}$. Both results are elementary.

2.8. Analytic facts about primes

The **prime-counting function** $\pi(x)$ is the number of primes at most x. We then have the prime number theorem, which is big enough of a deal that it got the name "prime number theorem":

Theorem. Prime number theorem. Citability: 4 Usefulness: 2

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

There are plenty of proofs of PNT you can find at the Wikipedia page, some of which are elementary. This is an *ineffective* result, because it's asymptotic. The PNT tells us that $\pi(2n) - \pi(n)$ is on the other of $n/\log n$ for sufficiently large n, but this is an ineffective result, whereas Bertrand is effective. There are many *effective* ways to state PNT, but I think the easiest to remember is Rosser's theorem:

Theorem. Rosser's theorem. Citability: 3 Usefulness: 1

The nth prime is at least $n \log n$.

The PNT is a foundational result of *analytic number theory*, in contrast to *algebraic number theory*, although the line between them is fuzzy. The earliest analytic result is probably Dirichlet's theorem, which we state using densities:

Theorem. Dirichlet's theorem (density). Citability: 3 Usefulness: 3

If a and d are relatively prime, then $\mathbb{P} \cap \{a + nd\}$ has density $\frac{1}{\varphi(d)}$.

I'll end with an observation. The "typical" first proof you learn of Dirichlet is quite analytic, drawing from complex analysis to look at L-functions and whatnot. But Dirichlet is also a consequence of Chebotarev, which needs algebraic number theory. Fuzzy lines, you know, fuzzy lines.

3. Nails

If I don't tell you which problems correspond to which theorems, then maybe this handout will be actually instructive? Who knows. Also, I make no promises that the theorems above will be helpful.

3.1. Box nails

1. (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. **Hint:** 3

2. (ISL 2000/N4) Find all triplets of positive integers (a, m, n) such that $a^m + 1$ divides $(a+1)^n$. **Hint:** 25

3. ([GG98]) Prove that $1, \dots, 2n$ can be partitioned into n pairs such that the sum of the numbers in each pair is prime. **Hint:** 13

4. (USAMO 2008/1) Prove that for each $n \in \mathbb{N}$, there are pairwise relatively prime $k_0, k_1, \dots, k_n$, all strictly greater than 1, such that $k_0 k_1 \dots k_n - 1$ is the product of two consecutive integers. **Hint:** 19

5. (↗) We call an integer p-*smooth* if its prime divisors are all at most p. For which p are there infinitely many pairs of consecutive p-smooth numbers? **Hint:** 11

6. (ISL 2011/N2) Let $d_1, \dots, d_9$ be distinct integers and let $P(x) = (x + d_1) \cdots (x + d_9)$. Prove there exists some N such that for all $x \geq N$, $P(x)$ is divisible by a prime larger than 20. **Hint:** 22

7. (IMO 2000/5) Does there exist $n \in \mathbb{N}$ such that n has exactly 2000 distinct prime divisors and $n \mid 2^n + 1$? **Hint:** 4

3.2. Common nails

8. (ISL 2009/N3) Let $f \colon \mathbb{N} \to \mathbb{N}$ be nonconstant, and suppose $a - b \mid f(a) - f(b)$ for all distinct $a, b \in \mathbb{N}$. Show that $\mathbb{P}\{f(n)\}$ is infinite. **Hint:** 8

9. (↗) Find all $f \in \mathbb{Z}[x]$ such that f is surjective modulo all sufficiently large primes. **Hint:** 18

10. (ISL 2014/N4) Let $n > 1$ be an integer. Prove that infinitely many terms of the sequence $\{a_k\}_{k \geq 1}$, defined by $a_k = \lfloor n^k / k \rfloor$ are odd. **Hint:** 7

11. (TSTST 2018/8) For which integers $b > 2$ do there exist infinitely many $n \in \mathbb{N}$ such that $n^2 \mid b^n + 1$? **Hint:** 15

12. (APMO 2021/2) For $P \in \mathbb{Z}[x]$ and $n \in \mathbb{N}$, let P_n be the number of positive integer pairs (a, b) such that $a < b \leq n$ and $n \mid |P(a)| - |P(b)|$. Find all $P \in \mathbb{Z}[x]$ such that $P_n \leq 2021$ for all $n \in \mathbb{N}$. **Hint:** 20

13. (USAMO 2013/5) Given $m, n \in \mathbb{N}$, prove there's some $c \in \mathbb{N}$ such that the numbers cm and cn have the same number of occurrences of each non-zero digit when written in base ten. **Hint:** 6

3.3. Drywall nails

14. (DeuX SL N4) Let $n \in \mathbb{N}$. Prove there exists some finite $S \subseteq \mathbb{N}$ such that:

    a) No element of S may be expressed as a^b for $a \geq 1$ and $b > 1$.

    b) For any prime p there exists $s \in S$ and $x \in \mathbb{Z}$ such that $x^n \equiv s \pmod{p}$.

    Hints: 12 27

15. (USAMO 2006/3) For $m \in \mathbb{Z}$, let $p(m)$ be the greatest prime divisor of m. By convention, we set $p(\pm 1) = 1$ and $p(0) = \infty$. Find all $f \in \mathbb{Z}[x]$ such that $\left\{p(f(n^2)) - 2n\right\}$ is bounded above. **Hints:** 24 17

16. (ISL 2011/N6) Let $P, Q \in \mathbb{Z}[x]$, such that if $R \in \mathbb{Z}[x]$ with $R(x) \mid P(x)$ and $R(x) \mid Q(x)$, then R is constant. Suppose that for every $n \in \mathbb{N}$, $P(n)$ and $Q(n)$ are positive, and $2^{Q(n)} - 1 \mid 3^{P(n)-1}$. Prove that Q is constant. **Hints:** 16 10

17. (USAMO 2012/3) For which integers $n > 1$ does there exist some $\{a_n\}$ of nonzero integers such that $a_k + 2a_{2k} + \cdots + na_{nk} = 0$ holds for every $k \in \mathbb{N}$? **Hints:** 14 26

18. (Balkan 2023/3) Let $N = 2023^{2023}$, and let $\omega(n)$ be the number of distinct prime divisors of n. Find all $P \in \mathbb{Z}[x]$, such that whenever $n \in \mathbb{N}$ with $\omega(n) > N$, then $P(n) \in \mathbb{N}$ with $\omega(n) \geq \omega(P(n))$. **Hints:** 1 9 21

19. (ISL 2019/N7$^+$) Prove there exist some $c > 0$ such that, for all $\varepsilon > 0$, there are infinitely many $n \in \mathbb{N}$ with the following property: there are infinitely many positive integers that cannot be expressed as the sum of fewer than $cn^{2-\varepsilon}$ pairwise coprime nth powers. **Hints:** 5 23 2

4. Hints

1. Set $P(x) = \alpha x^m Q(x)$; want to show Q constant.
2. Use PNT to show that N is large enough relative to n.
3. This is an application of anti-Schur.
4. Induct on 2000, base case $2^9 + 1$.
5. If all nth powers were 0 or 1 mod p^e, how many possible residues mod $\prod p^e$ do we get by summing m of them?
6. 142 857.
7. For even n, pick $p \in \mathbb{P}\big\{n^{n^r-1} - 1\big\}_{r\geq 1}$ and $k = n^r p$.
8. Let $N = f(1)\prod \mathbb{P}\{f(n)\}$, and consider $f(kN+1) - f(n)$.
9. Make $\omega(P(n))$ big relative to $\omega(n)$ by setting n as a product of specific primes.
10. Show that infinitely many primes divide $3^{P((a\operatorname{ord}_p(2), b\operatorname{ord}_p(3))} - 1$.
11. Imitate the Kobayashi proof.
12. The additive structure is unused, so take a primitive root mod p.
13. Construct so that most pairs sum to the same prime.
14. If we constrain $a_{ij} = a_i a_j$, we only need to define on primes.
15. Answer is all except $2^k - 1$. Compare IMO 2000/5.
16. What can you say about $P(n + a\operatorname{ord}_p(2) + b\operatorname{ord}_p(3))$?
17. Show that there's infinitely many n such that $p(f(n^2)) > 2n$.
18. Consider $f(x+1) - f(x)$.
19. Think about $f(x) = x^2 + x + 1$.
20. Apply problem 9.
21. Choose n, a product of $N+1$ primes, so $P(n) \equiv 0 \pmod{q_i}$ for N primes q_i.
22. This is an application of Kobayashi.
23. Set $n = 2\operatorname{lcm}(1, \ldots, x)$ and consider mod $N = \operatorname{lcm}(1, \ldots, 2x)$.
24. We can assume f is irred and nonconstant by factoring.
25. This is an application of Zsigmondy.
26. Examine the equation mod p, q for two primes in $[1, n]$.
27. If g is a primitive root mod p, then g^e is an nth power iff $e \equiv 0 \pmod{n}$.

5. Sketches

1. As $f(x) = x^p - p$ is irreducible, by anti-Schur there's some $q \in \mathbb{P} \setminus \mathbb{P}\{f(n)\}$ which works.

2. We have $(1, m, n)$ and $(a, 1, n)$. If a and m aren't 1, by Zsigmondy $a^m + 1$ has a primitive prime divisor, which does not divide $a + 1$, so $a^m + 1 \nmid (a + 1)^n$. Exception is $(2, 3, n)$.

3. By Bertrand some $2n + m$ is prime; pair up $\{m, \dots, 2n\}$ and recurse on $m - 1$.

4. Let $f(x) = x^2 + x + 1$. Pick $p_0, \dots, p_n \in \mathbb{P}\{f(n)\}$, which exist by Schur. Solve $f(x) \equiv 0 \pmod{p_i}$ by CRT.

5. None of them. Suppose there were consecutive numbers; write them as ax^3 and by^3 for a and b cubefree. We want $ax^3 - by^3 = 1$, which by Thue has finitely many solutions. Because they're p-smooth, there's only finitely many a and b.

6. In fact $P(x) = (x + a)(x + b)$ is enough. Let $\{s_n\}$ be the positive integers such that $P(s_n)$ is only divisible by primes smaller than 20. If $\{s_n\}$ is unbounded, then $\mathbb{P}\{s_n + a\}$ and $\mathbb{P}\{s_n + b\}$ are both finite, contradicting Kobayashi. Thus it's bounded and we're done.

   Remark: Here is an incorrect proof. Suppose that $\mathbb{P}\{P(n)\}$ was finite. By Kobayashi, if $\{n + a\}$ has finitely many prime divisors, then $\{n + b\}$ doesn't, contradiction. This doesn't work because it doesn't guarantee that *all* sufficiently large x are divisible by a prime larger than 20.

7. Yes. Define $\{a_n\}_1^{2000}$ as $a_1 = 9$ and $a_{n+1} = p_n a_n$ where p_n is a primitive prime divisor of $2^{a_n} + 1$, which exists by Zsigmondy. Then $n = a_{2000}$ works.

   Remark: Compare RMM 2014/4: Prove there are infinitely many n such that $n \mid 2^n + 1$ but $n \nmid 2^{2^n+1} + 1$.

8. Suppose $\mathbb{P}\{f(n)\} = \{p_1, \dots, p_n\}$. Suppose $f(1) = \prod p_i^{e_i}$. Take $N = f(1) \prod p_i$. Then $f(1) \mid kN \mid f(kN + 1) - f(1)$, so $f(1) \mid f(kN + 1)$. If $p_i^{e_i+1} \mid f(kN + 1)$, then $p_i^{e_i+1} \mid N$, and $p_i^{e_i+1} \mid f(1)$, contradiction. Hence $f(kN + 1) = f(1)$. Then $kN + 1 - n \mid f(kN + 1) - f(n) = f(1) - f(n)$, but the LHS is unbounded and the RHS is constant, and hence f must be constant too, contradiction.

   Remark: Compare ↗: Let $f \in \mathbb{Z}[x]$ be nonconstant with $f(0) \neq 0$. Show that $\mathbb{P}\{f(2^n)\}$ is infinite.

9. All $\deg f = 1$. If nonlinear, $g(x) = f(x + 1) - f(x)$ is nonconstant so by Schur $\mathbb{P}\{g(n)\}$ is infinite. For any $q \in \mathbb{P}\{g(n)\}$ we have $f(x + 1) \equiv f(x) \pmod{q}$ for some x which means f can't be surjective mod q.

10. For n odd, pick $p \mid n$; then all $k = p^m$ for sufficiently large m work. Several possible constructions for n even, here's two (sledgehammery) ones:

    - Pick large t and prime p with $p < 2^{2^t - t}(n/2)^{2^t} < 2p$ by Bertrand. Then $k = 2^t p$ works by checking mod p.
    - Pick $p \in \mathbb{P}\{n^{n^r-1} - 1\}_{r \geq 1}$, which is infinite by Kobayashi or Zsigmondy. We claim $k = n^r p$ works. Indeed, $n^k \equiv n^r \pmod{k}$, by checking both mod n^r and mod p.

11. All except $2^k - 1$. If $b = 2^k - 1$, suppose prime $p \mid n$. Then $b^{2n} \equiv 1 \pmod{p}$ so $\operatorname{ord}_p(b) \mid \gcd(2n, p-1) = 2$, so $p \mid b^2 - 1 = (b-1)(b+1)$. But as $b = 2^k - 1$, this forces $p \mid b - 1$, and hence $0 \equiv b^n + 1 \equiv 2 \pmod{p}$, contradiction.

    Else, a la IMO 2000/5, define $\{a_n\}$ by choosing odd prime $a_0 \mid b + 1$, and $a_{n+1} = p_n a_n$ where p_n is a primitive odd prime divisor of $b^{a_n} + 1$, which exists by Zsigmondy. Then all a_n work.

12. By problem 9, we must have $\deg P = 1$. Let $P(x) = cx + d$. If $p \mid c$, fix s and note $P(mp^s) \equiv P(mp^s + p^{2s-1}) \pmod{p^{2s}}$ for all m, contradiction for large s, hence $c = \pm 1$. WLOG $c = 1$; show that $d \geq -2021$ due to size.

13. Motivation: $c = 142\,857$ works often because of the decimal expansions of $\frac{1}{7}, \ldots \frac{6}{7}$ being cyclic shifts of each other. In particular, take some k and prime p such that $p \mid 10^k m - n$, which exists by Kobayashi. Then the expansions of $\frac{m}{p}$ and $\frac{n}{p}$ are shifts of each other; take c to be the repeating part of $\frac{1}{p}$.

14. Set $T = \{p_1, \ldots, p_n\} \subseteq \mathbb{P}$ and let $S = \{\prod T' \mid T' \subseteq T, T' \neq \varnothing\}$. For some $p \notin T$, let g be a primitive root and write $p_i = g^{e_i}$ for $e_i \in \{1, \ldots, p-1\}$. By pigeonhole two of the partial sums in $\{e_1 + \cdots + e_j\}_{j=1}^{n}$ are equal modulo n; their difference gives some $e_i + \cdots + e_j \equiv 0 \pmod{n}$ whence $g^{e_i + \cdots + e_j} \in S$ is a perfect nth power.

15. f must split into linear factors of the form $4n - a^2$. We can assume f is irred and nonconstant by factoring. By Schur, take some $p \in \mathbb{P}\{f(n^2)\}$, say $p \mid f(m^2)$. Then one of $m \bmod p$ or $p - (m \bmod p)$ is $< p/2$, so there's infinitely many n such that $f(n^2)$ has a prime divisor greater than $2n$.

    If the sequence was bounded above, there's some k such that $p(f(n^2)) - 2n = k$ has infinitely many solutions, implying $2x + k \mid f(x^2)$ as polynomials. As $f(x^2)$ is even, we must have $2x - k \mid f(x^2)$ too. Hence $f(x^2) = 4x^2 - k^2$ as it's irred, and $f(x) = 4x - k^2$.

16. Let $k = (P, Q)$, which is an integer. For prime p let $x_p = \operatorname{ord}_p(2)$ and $y_p = \operatorname{ord}_p(3)$. Note that $x_p \mid Q(n)$ iff $p \mid 2^{Q(n)} - 1$, and similarly for y_p. By Zsigmondy or Kobayashi, we can pick infinitely many such p; choose one of them.

    As $x_p \mid Q(n)$, we have $x_p \mid Q(n + ax_p)$ for any $a \in \mathbb{Z}$. Thus $p \mid 2^{Q(n+ax_p)} - 1 \mid 3^{P(n+ax_p)} - 1$, thus $y_p \mid P(n + ax_p)$, thus $y_p \mid P(n + ax_p + by_p)$ for any $b \in \mathbb{Z}$. As a special case, if $x_p \mid Q(n)$, then $y_p \mid P(n)$, which means that $\gcd(x_p, y_p) \mid \gcd(P(n), Q(n)) \mid k$, and so $(x_p, y_p) \leq k$.

    As $y_p \mid P(n)$ and $y_p \mid P(n + ax_p + by_p)$, we get $y_p \mid P(ax_p + by_p)$ as well, and thus $p \mid 3^{P(ax_p + by_p)} - 1$. By Bezout, we can pick a, b such that $ax_p + by_p = \gcd(x_p, y_p)$. But then we get infinitely many primes dividing $3^{P(\gcd(x_p, y_p))} - 1$, contradiction.

17. It's $n \geq 3$. We'll construct with $a_{ij} = a_i a_j$. Thus the sequence is determined by a_p for prime p, and we only need to have $a_1 + 2a_2 + \cdots + na_n = 0$. For large enough n, we can use Bertrand twice to pick primes $n/4 < p < n/2$ and $n/2 < q < n$. We'll then pick $a_r = 1$ for primes not p or q, and then pick a_p and a_q by Bezout. Casework is needed for which of p, $2p$, $3p$ are in range, plus more casework for small n.

18. Either $P(x) = x^m$ or $P(x) = c$ with $\omega(c) \le N+1$. Constant case is clear. Write $P(x) = \alpha x^m Q(x)$ with $Q(0) \neq 0$. If Q is constant, choosing n as the product of $N+1$ primes shows that $Q(x) = 1$.

    Suppose Q is nonconstant. By Schur, pick $q_1, \dots, q_T \in \mathbb{P}\{Q(n)\}$ for some $T \gg N$ such that $q_i > |Q(0)|$, and say $q_i \mid Q(a_i)$. By Dirichlet, pick N primes $p_i \equiv 1 \pmod{q_1 \cdots q_T}$ and by Dirichlet and CRT, pick prime $p_{N+1} \equiv a_i \pmod{q_i}$. Set $n = p_1 \cdots p_{N+1}$. We get $P(n) \equiv P(a_i) \equiv 0 \pmod{q_i}$, so $\omega(P(n)) \ge T \gg N$, contradiction.

19. Fix n. Suppose we have $N = p_1^{e_1} \cdots p_k^{e_k}$ such that $\varphi\left(p_i^{e_i}\right) \mid n$. Then all nth powers are 0 or 1 mod $p_i^{e_i}$, so the sum of m of them is $m-1$ or m, because the powers have to be pairwise coprime. By CRT there's at most $2^k m$ such numbers, so if $N > 2^k m$ then there's $N - 2^k m$ things modulo N that fail, giving infinitely many. Thus we want to find infinitely many n and N that work.

    Fix x. Let $n = 2\operatorname{lcm}(1, \dots, x)$ and $N = \operatorname{lcm}(1, \dots, 2x)$; we now need estimates. Note $2N/n > x^{\pi(2x)-\pi(x)}$, counting one for each prime in $(x, 2x]$. Similarly $n \le x^{\pi(x)}$. By PNT, we get, for sufficiently large x,

    $$\begin{aligned} \log\left(\frac{2N}{2^{\pi(2x)} n}\right) &> (\pi(2x) - \pi(x)) \log x - \pi(2x) \log 2 \\ &\ge (1-\varepsilon)\pi(x) \log x \\ &\ge (1-\varepsilon) \log(n), \end{aligned}$$

    and rearranging shows $N > 2^{\pi(2x)} n^{2-\varepsilon}$ as desired.

References

I've lowered the activation energy of reading the references by adding URLs, so maybe you'll look at them. Maybe. Also, I haven't even read all of these lol.

[AD12] Titu Andreescu and Gabriel Dospinescu. *Straight from the Book*. XYZ Press, 2012.

[BL06] Christian Ballot and Florian Luca. "Prime factors of $a^{f(n)} - 1$ with an irreducible polynomial $f(x)$". In: *New York J. Math* 12 (2006). https://nyjm.albany.edu/j/2006/12-3p.pdf, pp. 39–45.

[Bog18] Alexander Bogomolny. *Bertrand's Postulate*. https://www.cut-the-knot.org/arithmetic/algebra/BertrandPostulate.shtml. 2018.

[Dju07] Dusan Djukic. *Pell's equation*. http://refkol.ro/matek/mathbooks/Files/Pell-IMO.pdf. 2007.

[Els12] Christian Elsholtz. "Prime divisors of thin sequences". In: *The American Mathematical Monthly* 119.4 (2012). https://doi.org/10.4169/amer.math.monthly.119.04.331, pp. 331–333.

[Erd34] Paul Erdos. "A theorem of Sylvester and Schur". In: *Journal of the London Mathematical Society* 1.4 (1934). https://doi.org/10.1112/jlms/s1-9.4.282, pp. 282–288.

[GG98] L Greenfield and S Greenfield. "Some problems of combinatorial number theory related to Bertrands postulate". In: *J. Integer Seq* 1 (1998). https://cs.uwaterloo.ca/journals/JIS/green.html.

[Han73] Denis Hanson. "On a theorem of Sylvester and Schur". In: *Canadian Mathematical Bulletin* 16.2 (1973). https://doi.org/10.4153/cmb-1973-035-3, pp. 195–199.

[HS13] Marc Hindry and Joseph H Silverman. *Diophantine Geometry: An Introduction*. Vol. 201. Springer Science & Business Media, 2013.

[Kob81] Hiroshi Kobayashi. "On existence of infinitely many prime divisors in a given set". In: *Tokyo Journal of Mathematics* 4.2 (1981). https://doi.org/10.3836/tjm/1270215162, pp. 379–380.

[Mic14] Bart Michels. *Zsigmondy's Theorem*. https://pommetatin.be/files/zsigmondy_en.pdf. 2014.

[Mor90] Patrick Morton. "Musings on the prime divisors of arithmetic sequences". In: *The American Mathematical Monthly* 97.4 (1990). https://doi.org/10.1080/00029890.1990.11995599, pp. 323–328.

[Qui19] Carl Joshua Quines. *Nineteen proofs there are infinitely many primes*. https://cjquines.com/files/infiniteprimes.pdf. 2019.

[Sch11] Dan Schwarz. *Kobayashi's theorem*. https://aops.com/community/c6h362152p2525061. 2011.

[Yab01] Minoru Yabuta. "A simple proof of Carmichael's theorem on primitive divisors". In: *Fibonacci Quarterly* 39.5 (2001). https://fq.math.ca/Scanned/39-5/yabuta.pdf, pp. 439–443.

Acknowledgements

Thanks to tenth, Wayne Zhao, and Zi Song Yeoh for comments.

A. Diophantine geometry

One of the big ideas is that classifying by degree is insufficient, and the morally correct way is to classify based on the *genus*, which is a geometric property. Say we had some $f \in \mathbb{Z}[x, y]$. The graph defined by $f(x, y) = 0$ over $\mathbb{R}^2$ is the *affine curve* of f, and say it has degree $d = \deg f$. We can then homogenize it to get some ${}^h f \in \mathbb{Z}^d[x, y, z]$, by setting ${}^h f(x, y, z) = z^d f(x/z, y/z)$. For example, $x^4 + y^4 - 1$ homogenizes to $x^4 + y^4 - z^4$. The graph defined by ${}^h f(x, y, z) = 0$ over $\mathbb{RP}^2$ is a *projective curve*. Here, $\mathbb{RP}^2$ is the real projective plane, the set of points (x, y, z) with $x + y + z = 1$.[2]

We check if there are any *singularities* on ${}^h f$, which is a point on the projective curve that is 0 for each partial derivative $\partial^h f/\partial x$, $\partial^h f/\partial y$, $\partial^h f/\partial z$. Our example, $x^4 + y^4 - z^4$, has no singularities; we say it is *nonsingular*. If it did have singularities, we'd use a procedure to *resolve* the singularities, such as *blowing up*. Because it's nonsingular, we can compute the *genus* as $g = \binom{d-1}{2} = 3$. We count the number of *points at infinity*, which are points with $z = 0$; this gives us the *Euler characteristic*, which is $\chi = 2 - 2g - (\#\text{ of points at infinity}) = -4$.

The integer solutions to $f(x, y) = 0$ are classified by χ. If $\chi > 0$ it's an infinite set, common in the $d = 2$ case. If $\chi = 0$ it's a finitely generated group, as with elliptic curves. If $\chi < 0$ it's a finite set, like in our case. This statement includes the Mordell–Weil, Siegel, and Falting theorems; together with Roth these are four of the fundamental theorems in Diophantine geometry. I picked this up from a book I didn't read: [HS13].

[2] You can scale by some constant k, because if ${}^h f(x, y, z) = 0$ then ${}^h f(kx, ky, kz) = 0$ because ${}^h f$ is homogeneous. If you've seen barycentric coordinates, this should look familiar.