1. PROOFS THAT THERE ARE INFINITELY MANY PRIMES

Introduction

The *fundamental theorem of arithmetic* states that every positive integer may be factored into a product of primes in a unique way. Moreover any finite product of prime numbers equals some positive integer. Therefore there is a 1-to-1 correspondence between positive integers and finite products of primes. Thus we can understand positive integers by decomposing them into their prime factors and studying these, just as we can understand molecules by studying the atoms of which they are composed.

Once one begins to determine which integers are primes and which are not, one quickly finds that there are many of them, though as we go further and further, they seem to be a smaller and smaller proportion of the positive integers. It is also tempting to look for patterns amongst the primes: Can we find a formula that describes all of the primes? Or at least some of them? Are there actually infinitely many? And, if so, can we quickly determine how many there are up to a given point? Or at least give a good estimate? Once one has spent long enough determining primes, one cannot help but ask whether it is possible to recognize prime numbers quickly and easily? These questions motivate the early parts of this course.

1. Proofs that there are infinitely many primes, without analysis

1.1. Euclid and beyond. Ancient Greek mathematicians knew that there are infinitely many primes. Their beautiful proof by contradiction goes as follows: Suppose that there are only finitely many primes, say k of them, which we will denote by $2 = p_1 < p_2 = 3 < \ldots < p_k$. What are the prime factors of $p_1p_2 \ldots p_k + 1$? Since this number is > 1 it must have a prime factor, and this must be p_j for some j, $1 \le j \le k$ (since *all* primes are contained amongst $p_1, p_2, \ldots, p_k$). But then p_j divides both $p_1p_2 \ldots p_k$ and $p_1p_2 \ldots p_k + 1$, and hence p_j divides their difference, 1, which is impossible.[1]

Many people dislike this proof, since it does not exhibit infinitely many primes, but only shows that it is impossible that there are finitely many. It is possible to more-or-less correct this deficiency by defining the sequence $a_1 = 2, a_2 = 3$ and then $a_n = a_1a_2 \ldots a_{n-1} + 1$ for each $n \ge 2$. Let p_n be some prime divisor of a_n. We claim that the p_n are all distinct so we have an infinite sequence of distinct primes. We know that these primes are distinct else

[1]Euclid gives this proof in Book 9 Proposition 20 of his *Elements*, assuming that there are just three primes. The reader is evidently meant to infer that the same proof works no matter how large a finite number of primes we assume there to be. The notation of those times was far less flexible than that of today, so that the astute reader necessarily had to deduce the full content of the statement of a theorem, or of a proof, from what was written, and could not necessarily learn all that was meant from what was actually written. Even Renaissance thinkers like Fermat and Descartes recognized this difficulty and deplored those who could not navigate it adroitly.

if $p_m = p_n$ with $m < n$ then p_m divides $(a_m, a_n) = (a_m, 1) = 1$, since $a_n \equiv 1 \pmod{a_m}$ by our construction, which is impossible.

Fermat conjectured that the integers $b_n = 2^{2^n} + 1$ are primes for all $n \geq 0$. His claim starts off correct: $3, 5, 17, 257, 65537$ are all prime, but is false for $b_5 = 641 \times 6700417$, as Euler famously noted. Nonetheless we can prove that if p_n is some prime divisor of b_n for each $n \geq 0$ then $p_0, p_1, \ldots$ is an infinite sequence of distinct primes, in this case because $b_n = b_1 b_2 \ldots b_{n-1} + 2$ for each $n \geq 1$, and so $(b_m, b_n) = (b_m, 2) = 1$ for all $m < n$, since $b_n \equiv 2 \pmod{b_m}$.[2]

A related proof involves letting q_n be the smallest prime factor of $n! + 1$. Thus there cannot be a largest prime n since q_n must be a larger prime.

Exercises

1.1a. (Other proofs inspired by Euclid's proof) Suppose that we are given distinct primes $p_1, p_2, \ldots, p_k$, and let m denote their product, $p_1 p_2 \ldots p_k$. Show that *each* of the following integers N has a prime factor which is not equal to any prime in this list, and so deduce that there are infinitely many primes.

a) For any $r, 1 \leq r \leq k$ let $n = p_1 p_2 \ldots p_r$ and $N := n + m/n$.

b) (Reminiscent of proofs of the Chinese Remainder theorem): Let $N := \sum_{i=1}^{k} m/p_i$.

1.1b. In this question we give an algorithm that determines all of the primes.

a) Let $p_1, p_2, \ldots, p_k$ be distinct primes, with $m = p_1 p_2 \ldots p_k$. Prove that if $N = \sum_{i=1}^{k} N_i$, where the prime factors of N_i are exactly $\{p_1, p_2, \ldots, p_k\} \setminus \{p_i\}$ for each i, then $(N, m) = 1$.

b) For any given integer N with $(N, m) = 1$, use the Chinese Remainder theorem to determine integers M_i for which $N \equiv \sum_{i=1}^{k} M_i \pmod{m}$, where the prime factors of M_i are exactly $\{p_1, p_2, \ldots, p_k\} \setminus \{p_i\}$ and $1 \leq M_i \leq m$, for each i.

c) Prove that if $1 \leq N \leq \sum_{i=1}^{k} m/p_i$ with $(N, m) = 1$ then there exist integers N_i as in part a, with each $|N_i| \leq m$. (Hint: One idea is to select M_i or $M_i - m$ in part b).

d) Taking $p_1, p_2, \ldots, p_k$ to be the primes up to $\sqrt{x}$ we have a way to determine, with proof, each prime N between $\sqrt{x}$ and x by finding a representation of N as in part c. Find all the primes between 5 and 100 in this way, along with these proofs that they are indeed prime.

1.1c. Use the sequence of Fermat numbers to prove that, for each integer $k \geq 1$, there are infinitely many primes $\equiv 1 \pmod{2^k}$.

1.1d. Suppose that $p_1 = 2 < p_2 = 3 < \ldots$ is the sequence of prime numbers. Use the fact that every Fermat numbers has a distinct prime divisor to prove that $p_n \leq 2^{2^n} + 1$. What can one deduce about the number of primes up to x?

1.1e. (Open questions). Are there infinitely many primes of the form a_n? If $p_1 = 2 < p_2 = 3 < \ldots$ is the sequence of prime numbers then are there infinitely many n for which $p_1 p_2 \ldots p_n + 1$ is prime? For which $p_1 p_2 \ldots p_n - 1$ is prime? Let us determine an infinite sequence of primes by starting with prime q_1, and then letting q_n be some prime divisor of

[2]This proof appeared in a letter from Goldbach to Euler in July 1730.

$q_1q_2\dots q_{n-1}+1$. Can this be arranged so that the sequence $q_1, q_2, ...$ is a re-arrangement of the set of all primes? What if q_n is the smallest prime divisor of $q_1q_2\dots q_{n-1}+1$?

1.2. Various other non-analytic proofs.

The *Mersenne numbers* take the form $M_n = 2^n - 1$. Suppose that p is prime and q is a prime dividing $2^p - 1$. The order of 2 mod q, must be divisible by p, and must divide $q-1$, hence $p \le q-1$. Thus there cannot be a largest prime p, since any prime factor q of M_p is larger, and so there are infinitely many primes.

Furstenberg gave an extraordinary proof using point set topology: Define a topology on the set of integers $\mathbb{Z}$ in which a set S is open if it is empty or if for every $a \in S$ there is an arithmetic progression $\mathbb{Z}_{a,q} := \{a + nq : n \in \mathbb{Z}\}$ which is a subset of S. Evidently each $\mathbb{Z}_{a,q}$ is open, and it is also closed since $\mathbb{Z}_{a,q} = \mathbb{Z} \setminus \cup_{b:\ 0\le b\le q-1,\ b\ne a}\mathbb{Z}_{b,q}$. If there are only finitely many primes p then $A = \cup_p \mathbb{Z}_{0,p}$ is also closed, and so $\mathbb{Z} \setminus A = \{-1, 1\}$ is open, but this is obviously false since A does not contain any arithmetic progression $\mathbb{Z}_{1,q}$. Hence there are infinitely many primes.

Exercises

1.2a. a) Prove that if $f(t) \in \mathbb{Z}[t]$ and $r, s \in \mathbb{Z}$ then $r - s$ divides $f(r) - f(s)$.

b) Prove that if $2^n - 1$ is prime then n is prime.

c) Prove that if $2^n + 1$ then n is either 0 or a power of 2.

1.2b. Prove that if prime q divides $2^p - 1$, where p is prime, then 2 has order p mod q. Deduce that $(2^p - 1, 2^\ell - 1) = 1$ for all primes p and ℓ.

1.2c. (Open questions). Prove that there are infinitely many Mersenne primes, $2^p - 1$. (This is equivalent to asking whether there are infinitely many even perfect numbers, since n is an even perfect number if and only if it is of the form $2^{p-1}(2^p - 1)$ with $2^p - 1$ prime.) Prove that there are infinitely many Fermat primes, $2^{2^n} + 1$. Prove that there are integers n for which $2^{2^n} + 1$ is composite.[3]

1.2d. (Open). Prove that there are infinitely primes p for which $2^p - 1$ is composite. (This is a conjecture because one can prove, and you should prove, that if $p \equiv 3 \pmod 4$ and $q = 2p + 1$ is also prime then q divides $2^p - 1$, so that $2^p - 1$ is composite.)

1.2e. We know that

$$2^2 - 1,\ 2^{2^2-1} - 1,\ 2^{2^{2^2-1}-1} - 1 \text{ and } 2^{2^{2^{2^2-1}-1}-1} - 1$$

are all prime and it is an open question as to whether any terms in this sequence are composite?

1.3. Primes in certain arithmetic progressions. Any prime $\equiv a \pmod m$ is divisible by (a, m), and so if $(a, m) > 1$ there cannot be more than one prime $\equiv a \pmod m$.

[3]There are no primes known of the form $2^{2^n} + 1$ other than for $n \le 4$, and we know $2^{2^n} + 1$ is composite for $5 \le n \le 30$ and many other n besides. It is always a significant moment when a Fermat number is factored for the first time.

Thus all but finitely many primes are distributed among the $\phi(m)$ arithmetic progressions $a \pmod m$ with $(a,m)=1$. We will eventually prove that all such arithmetic progressions contain infinitely many primes, and that the primes are roughly equally distributed amongst these $\phi(m)$ arithmetic progressions $\pmod m$. For now we will prove results along these lines using only very elementary methods. We begin by proving that there are infinitely many primes in each of the two feasible residue classes mod 3.

There are infinitely many primes $\equiv -1 \pmod 3$, for if there are only finitely many, say $p_1, p_2, \dots, p_k$, then $N = 3p_1p_2\dots p_k - 1$ must have a prime factor $q \equiv -1 \pmod 3$, else $N \equiv 1 \pmod 3$, and so q divides both N and $N+1$ and hence their difference 1, which is impossible. A similar proof works for primes $\equiv -1 \pmod 4$, and indeed for much more general sets of primes – see exercise 1.3a below.

How about the primes $\equiv 1 \pmod 3$? We can look for sequences of integers n, *all* of whose prime factors q are $\equiv 1 \pmod 3$, by the idea of exercise 1.2b: that is, for each such n there should be some integer a, such that the order of $a \bmod q$ must be divisible by 3, for each q which divides n. Now if a has order 3 then $a^3 \equiv 1 \pmod q$, and to avoid order 1 we want $a \not\equiv 1 \pmod q$. We come close to this by considering the prime factors of $(a^3-1)/(a-1) = a^2+a+1$: the only way a prime factor of this can have order 1 is if it divides $(a^2+a+1, a-1) = (3, a-1)$, that is the prime factor must be 3 and $a \equiv 1 \pmod 3$. We are ready to prove that there are infinitely many primes $\equiv 1 \pmod 3$: If there are only finitely many, say $p_1, p_2, \dots, p_k$, then $a = 3p_1p_2\dots p_k$ has order 3 modulo any prime divisor q of $N = a^2+a+1$ so that $q \equiv 1 \pmod 3$, but then q divides N, and a which divides $N-1$, and hence their difference, 1, which is impossible.

In order to generalize this argument to primes $\equiv 1 \pmod m$, we need to replace the polynomial a^2+a+1 be one that recognizes when a has order m. Evidently this must be a divisor of the polynomial a^m-1, indeed a^m-1 divided through by all of the factors corresponding to orders which are proper divisors of m. So let define the *cyclotomic* polynomials $\phi_n(t) \in \mathbb{Z}[t]$, inductively, by the requirement $t^m - 1 = \prod_{d|m} \phi_d(t)$ for all $m \geq 1$, with each $\phi_d(t)$ monic. The roots of t^m-1 are the distinct mth roots of unity, so our definition implies that the roots of $\phi_m(t)$ are exactly the *primitive* mth roots of unity, that is those $\alpha \in \mathbb{C}$ for which $\alpha^m = 1$ but $\alpha^r \neq 1$ for all r, $1 \leq r \leq m-1$. These can be written more explicitly as $\exp(2i\pi j/m)$ with $(j,m)=1$ so that $\phi_m(t)$ has degree $\phi(m)$.

Exercises

1.3a. Let G be a proper subgroup of the multiplicative group of elements mod m (that is, the residue classes coprime to m).

a) Show that if N is an integer with $(N,m)=1$ where N is not an element of G, then N has a prime factor which is not an element of G.

b) Given any finite set of primes $p_1, p_2, \dots, p_k$ which do not divide m, and a residue class $b \pmod m$, show that for any $b \in (\mathbb{Z}/m\mathbb{Z})^* \setminus G$ there exists an integer N such that $N \equiv b \pmod m$ and $(N, p_1p_2\dots p_k) = 1$.

c) We will now prove that there are infinitely many primes whose residues mod m which do not belong to the subgroup G. For if there are only finitely many, say $p_1, p_2, \dots, p_k$, select N as in part b, and then use part a to deduce the desired conclusion.

d) Deduce that there are infinitely many primes in at least two of the arithmetic progressions 3 mod 8, 5 mod 8, and 7 mod 8.

1.3b. a) Prove that the set of *primitive* mth roots of unity can be written in the form $\exp(2i\pi j/m)$ with $(j,m)=1$.

b) p is a *primitive prime factor* of a^m-1 if p divides a^m-1 but p does not divide a^n-1 for any $n, 1\le n\le m-1$. Show that every primitive prime factor of a^m-1 divides $\phi_m(a)$.

c) Prove that $\gcd(a^m-1,a^n-1)=a^{(m,n)}-1$. Deduce that if prime p divides $\phi_m(a)$ but is not a primitive prime factor of a^m-1 then p divides $\phi_d(a)$ for some proper divisor, d, of m.

d) Prove that if d is a proper divisor of m and prime p divides $\gcd(\phi_m(a),\phi_d(a))$ then m/d is a power of p. (Hint: If prime $q\ne p$ divides m/d consider $(a^m-1)/(a^{m/q}-1) \pmod{a^{m/q}-1}$, and establish that $\phi_d(a)$ divides $a^{m/q}-1$.)

e) Prove that $\phi_m(0)=1$ for all $m>1$. Deduce that if p is a prime factor of $\phi_m(ma)$ for any integer a then $p\equiv 1 \pmod m$.

f) Use part e to deduce that there are infinitely primes $\equiv 1 \pmod m$.

1.3c. We use the theory developed in exercise 1.3b in another question.

a) Writing $a^d=1+kp^r$ where $p\nmid k$, prove that if $p^r\ne 2$ then $a^{pd}-1$ is divisible by p^{r+1} but not by p^{r+2}. Deduce that if p divides $\phi_m(a)$ but is not a primitive prime factor of a^m-1 then p^2 does not divide $\phi_m(a)$, except when $m=2$ and $a\equiv 3 \pmod 4$.

b) Use 1.3b.d and 1.3c.a to show that if $m>2$ and a^m-1 does not have a primitive prime factor then $\phi_m(a)$ divides m.

c) By proving upper and lower bounds on $|\phi_m(a)|$, show that $|\phi_m(a)|>m$ for all integers a and m with $|a|\ge 2$ and $m\ge 3$, except $\phi_3(-2)=\phi_6(2)=3$. (Hints: If $|a|\ge 3$ then $|\phi_m(a)|=\prod_{(j,m)=1}|a-\exp(2i\pi j/m)|\ge(|a|-1)^{\phi(m)}$ for $m\ge 3$ except when $|a|=3$ and $m=4$ or 6. When $|a|=2$ use only those roots of unity in the other half of the unit circle from a.)

d) Finally deduce that for each integer a with $|a|\ge 2$, the integers $(a^m-1)/(a-1)$ have a primitive (and thus distinct) prime factor for all integers $m\ne 1,2$ or 6.

$\{x_n\}_{n\ge 0}$ is a *Lucas sequence* if $x_0=0, x_1=1$ and

$$x_{n+2}=bx_{n+1}+cx_n \quad \text{for all} \quad n\ge 0, \tag{1}$$

for given non-zero, coprime integers b,c; the integers $x_n=(a^n-1)/(a-1)$ form a Lucas sequence with $b=a+1$ and $c=-a$ for each $n\ge 0$. In 1913 Carmichael showed that if the discriminant $\Delta:=b^2+4c>0$ then x_n has a primitive prime factor for each $n\ne 1,2$ or 6 except for $F_{12}=144$ where F_n is the Fibonacci sequence ($b=c=1$), and for F'_{12} where $F'_n=(-1)^{n-1}F_n$ ($b=-1,\ c=1$). It is much more difficult to prove that Lucas sequences with negative discriminant have primitive prime factors. Nonetheless, in 1974 Schinzel succeeded in showing that x_n has a primitive prime factor once $n>n_0$, for some sufficiently large n_0, if $\Delta\ne 0$, other than in the periodic case $b=\pm 1,\ c=-1$. Determining the smallest possible value of n_0 has required great efforts culminating in the beautiful work of Bilu, Hanrot and Voutier [BHV] who proved that $n_0=30$ is best possible (indeed if $b=1, c=-2$ then $x_5,\ x_8,\ x_{12},\ x_{13},\ x_{18},\ x_{30}$ have no primitive prime factors).

1.3d. In exercise 1.3b.f we saw that there are infinitely many primes $\equiv 1 \pmod 8$, and in exercise 1.3a.d that there are infinitely many primes i at least two of the other arithmetic progressions $\pmod 8$.

a) For $b = 3, 5$ or -1 suppose that there are only finitely many primes $\equiv b \pmod 8$, and let n_b be their product. Establish a contradiction by considering the prime factors of $n_b^2 + b - 1, n_b^2 + 4$ or $n_b^2 - 2$, respectively. (Hint: Use the law of quadratic reciprocity.)

b) Generalize this argument to prime divisors of values of other quadratic polynomials.

1.4. Prime divisors of polynomials. We know that any linear polynomial $mt+a \in \mathbb{Z}[t]$ with $(m, a) = 1$ takes on infinitely many prime values (which is equivalent to the fact that there are infinitely many primes $\equiv a \pmod m$ if $(a, m) = 1$). We wish to generalize this to any irreducible $f(t) \in \mathbb{Z}[t]$, with suitable restrictions. To formulate the restrictions there is one subtlety: the reason we need $(m, a) = 1$ in the linear case is that (m, a) divides $mn + a$ for every integer n, and in fact $(m, a) = \gcd\{mn + a : \ n \in Z\}$. Hence let us define Content(f) to be the gcd of the integers $f(n)$ as we vary over $n \in \mathbb{Z}$. It is conjectured that for any irreducible $f(t) \in \mathbb{Z}[t]$ with Content$(f) = 1$ there are infinitely many integers n for which $f(n)$ is prime. (In fact that for any irreducible $f(t) \in \mathbb{Z}[t]$ there are infinitely many integers n for which $f(n)/\text{Content}(f)$ is prime.)

The polynomial $n^2 + n + 41$ is prime for $n = 0, 1, \dots, 39$, though composite for $n = 40$. One can ask whether there are any polynomials $f(t) \in \mathbb{Z}[t]$ such that $f(n)$ is prime for all integers n? The answer is no: We now show that if $f(t) \in \mathbb{Z}[t]$ has degree ≥ 1 then $f(n)$ is composite for infinitely many integers n. Since a non-zero polynomial has only finitely many roots, for example $(f(t) - 1)f(t)(f(t) + 1)$, thus $|f(n)| \geq 2$ for all but finitely many integers n. Select any such n and let $m = f(n)$. Now $f(n + km) \equiv f(n) \equiv 0 \pmod m$ for any integer k, by exercise 1.2a.a, so that $f(n + km)$ is composite all k except for the finitely many $n + km$ which are roots of $(f(t) - m)f(t)(f(t) + m)$.

One can use a minor variation to show that if $f(t) \in \mathbb{Z}[t]$ has degree d and there are more than $2d$ distinct integers n for which $|f(n)|$ is prime then $f(t)$ is irreducible. To prove this suppose $f(t) = g(t)h(t)$; for each n where $|f(n)|$ is prime we have that either $g(n) = \pm 1$ or $h(n) = \pm 1$. Now there are no more than $2 \deg(g)$ roots of $(g(t) - 1)(g(t) + 1)$, and no more than $2 \deg(h)$ roots of $(h(t) - 1)(h(t) + 1)$, and therefore $\leq 2 \deg(g) + 2 \deg(h) = 2d$ distinct integers n for which $|f(n)|$ prime. (The "$2d$" in this result can be improved to "$d + 2$", and this is probably best possible for all $d \geq 6$. If we ask for $f(n)$ to be prime then the correct bound is d.)

We finish this section by proving that for any $f(t) \in \mathbb{Z}[t]$ of degree ≥ 1 there are infinitely many distinct primes p for which p divides $f(n)$ for some integer n. We may assume that $f(n) \neq 0$ for all $n \in \mathbb{Z}$ else we are done. Now suppose that $p_1, \dots, p_k$ are the only primes which divide values of f and let $m = p_1 \dots p_k$. Then $f(nmf(0)) \equiv f(0) \pmod{mf(0)}$ for every integer n, by exercise 1.2a.a, so that $f(nmf(0))/f(0) \equiv 1 \pmod m$. Therefore $f(nmf(0))$ has prime divisors other than those dividing m for all n but the finitely many n which are roots of $(f(tmf(0)) - f(0))(f(tmf(0)) + f(0))$, a contradiction.

Exercises

1.4a. a) Prove that the gcd of the coefficients of f divides Content(f).

b) Give an example to show that Content(f) can be larger than the gcd of the coefficients of f.

c) If a polynomial $f(t) \in \mathbb{Z}[t]$ has degree d then show that there exist integers $b_0, b_1, \dots, b_d$ for which $f(t) = \sum_{j=0}^{d} b_j \binom{t}{j}$.

d) Prove that Content(f) $= \gcd_{0\le j\le d} b_j = \gcd_{0\le n\le d} f(n)$.

1.4b. Use the proof above to show that if f has degree d then there exists an integer n, with $|n| \le d(1 + \max_{|m|\le d} |f(m)|)$, for which $f(n)$ is composite. Can you significantly improve this?

1.4c. Suppose that $m_1, m_2, \dots, m_k$ are a set of pairwise coprime integers such that m_j divides $f(a_j)$ for some integer a_j, for each j. Prove that there are infinitely many integers n for which $m_1 m_2 \dots m_k$ divides $f(n)$.

1.4d.a) Suppose that $g(t) \in \mathbb{Z}[t]$, where $m_1, \dots, m_k$ are integers that satisfy $g(m_i) = 1$, and $n_1, \dots, n_\ell$ are integers that satisfy $g(n_j) = -1$. Prove that $\prod_{i=1}^{k}(m_i - n_j)$ divides 2 for each j, and $\prod_{j=1}^{\ell}(m_i - n_j)$ divides 2 for each i.

b) Deduce that if $k, \ell \ge 1$ then we must have $g(x) = \pm G(\pm x + a)$ for some choice of sign $\pm$ and some integer a where $G(x)$ is either $x(x-1)(x-3)+1$ with $k = 3, \ell = 1$, or $x(x-1)-1$ with $k = \ell = 2$, or $2x^2 - 1$ with $k = 2, \ell = 1$, or $2x - 1$ with $k = \ell = 1$, or $x - 1$ with $k = \ell = 1$.

c) Suppose that $f(t) \in \mathbb{Z}[t]$ is reducible of degree d, for which there are more than d integers n with$|f(n)|$ is prime. Deduce that $f(t)$ has a proper factor $g(t)$, as in part b.

d) Suppose that $f(t) \in \mathbb{Z}[t]$ is reducible of degree d, for which there are $\ge d + 4$ integers n for which $|f(n)|$ is prime. Deduce that there exist integers a and b such that $f(t) = g(t + b)$ where $g(t) = ((t - a)(t - a - 1) - 1)(t^2 - t - 1)$ so that the prime values are $g(2) = g(a-1) = a^2 - 3a + 1, -g(1) = -g(a) = a^2 - a - 1, -g(0) = -g(a+1) = a^2 + a - 1$ and $g(-1) = g(a + 2) = a^2 + 3a + 1$.

Hence there are examples of reducible polynomials of degree four, taking on prime values eight times, in fact there is an example for each a such that $h(t) := (t-a)(t-a-1) - 1$ is prime for $t = -1, 0, 1$ and 2, something which we have conjectured above happens infinitely often, for instance for $a = 4$.

e) Our conjecture implies that there is an infinite sequence of integers $r_1, r_2, \dots$ such that $r_i^2 + r_i - 1$ is prime for each i. For a given integer $d \ge 2$, let $f(t)$ be the polynomial $(t^2 - t - 1)(1 + a\prod_{i=1}^{d-2}(t + r_i))$. The *prime k-tuplets conjecture* states that if $a_1 t + b_1, \dots, a_k t + b_k \in \mathbb{Z}[t]$ have the property that Content$(\prod_{j=1}^{k}(a_j t + b_j)) = 1$ then there are infinitely many integers n for which $a_1 n + b_1, \dots, a_k n + b_k$ are all prime. Use the prime k-tuplets conjecture to deduce that there exist integers a such that $|f(t)|$ takes on prime values at $d + 2$ different integer values for t (and, in fact, $f(t)$ takes on prime values at d different integer values for t). Show that these examples give the most possible prime values, for large enough d.

If one asks for prime values of $f(n)$/Content(f) then the answer is surprisingly different: The number of prime values that can be taken by $f(n)$/Content(f) where $f(t) \in \mathbb{Z}[t]$ is a

reducible polynomial of degree d is something like $2^{cd/\log d}$, for some constant $c > 0$. See [ChRu] for details.

1.4e.a) For a given polynomial $f(t) = \sum_{i=0}^{d} a_i t^i \in \mathbb{Z}[t]$ define $H := \max_{0 \le i \le d-1} |a_i/a_d|$. Show that if $f(\alpha) = 0$ then $|\alpha| < H + 1$.

b) Show that if f is reducible and n is an integer for which $|f(n)|$ is prime then there exists a root α of $f(\alpha) = 0$ for which $|n - \alpha| \le 1$.

c) Deduce that if n is an integer, with $|n| \ge H + 2$, for which $|f(n)|$ is prime then $f(t)$ is irreducible.

d) Modify this argument to show that if n is an integer, with $|n| \ge H + 1 + \text{Content}(f)$, for which $|f(n)/\text{Content}(f)|$ is prime then $f(t)$ is irreducible.

e) Modify this argument to show that if prime $p = a_0 + a_1 10 + \ldots + a_d 10^d$ in base 10 then the polynomial $a_0 + a_1 t + \ldots + a_d t^d$ is irreducible. (Hint: Prove first that, for α as in part b, we have $|f(\alpha)/\alpha^d| \ge \text{Re}(a_d + a_{d-1}/\alpha) - 9 \sum_{j \ge 2} 1/|\alpha|^j$, and then that $\text{Re}(1/\alpha) > 0$.)

1.5. A DIVERSION: DYNAMICAL SYSTEMS PROOFS. In general we know that the prime divisors of a sequence of integers > 1 form an infinite sequence of primes if the integers in the sequence are pairwise coprime. We will generalize the constructions from section 1.1. We begin by simplifying the description of the sequences a_n and b_n.

$$a_{n+1} - 1 = a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_{n-1}) a_n = (a_n - 1) a_n,$$

so that $a_{n+1} = f(a_n)$ where $f(t) := t^2 - t + 1$. (Similarly $b_{n+1} = g(b_n)$ where $g(t) := t^2 - 2t + 2$.) How do we explain the fact that $a_n \equiv 1 \pmod{a_m}$ for all $m < n$? Well $a_{m+1} = f(a_m) \equiv f(0) = 1 \pmod{a_m}$ and, thereafter, $a_{n+1} = f(a_n) \equiv f(1) = 1 \pmod{a_m}$ by induction on $n \ge m + 1$. (Similarly $b_{m+1} = g(b_m) \equiv g(0) = 2 \pmod{b_m}$ and $b_{n+1} = g(b_n) \equiv g(2) = 2 \pmod{b_m}$ by induction.) So the only requirements on f_1 seem to be that $f(0) = f(1) = 1$, and f is the simplest such polynomial is $1 + t(t-1)$. In fact any polynomial $1 + h(t)t(t-1)$, where $h(t) \in \mathbb{Z}[t]$ has positive leading coefficient, will work. In section 1A1 we will determine *all* polynomials $f(t) \in \mathbb{Z}[t]$ that be used into this framework.

We introduce a little terminology from dynamical systems: A number a is said to be *preperiodic* for f, if the sequence $a, f(a), f(f(a)), \ldots$ is eventually periodic.

Proposition 1.5.1. *Let $f(t) \in \mathbb{Z}[t]$ have degree > 1, positive leading coefficient, and $f(0) \ne 0$. Suppose that 0 is a preperiodic point for f but that 0 is not part of the period, and let ℓ be the least common multiple of the integers in the sequence $f(0), f(f(0)), f(f(f(0))), \ldots$. If $a_0 \in \mathbb{Z}$ with $a_{n+1} = f(a_n)$ for all $n \ge 0$, and $(a_n, \ell) = 1$ for all $n \ge 0$, then we obtain an infinite sequence of distinct primes by selecting one prime factor from each a_n.*

Proof. Let $w_0 = 0$ and $w_{n+1} = f(w_n)$ for all $n \ge 0$, so that $a_{m+1} = f(a_m) \equiv f(0) = w_1 \pmod{a_m}$ and, thereafter, $a_{m+j+1} = f_1(a_{m+j}) \equiv f(w_j) = w_{j+1} \pmod{a_m}$ by induction on $j \ge 1$. Therefore if $m < n$ then $(a_m, a_n) = (a_m, w_{n-m})$ which divides (a_m, ℓ), which equals 1 by the hypothesis. The rest of the proof follows as above.

To be able to use Proposition 1.5.1 we need a good idea of when 0 is a preperiodic point, which turns out to be simpler than one might guess:

Proposition 1.5.2. *Suppose that $f(t) \in \mathbb{Z}[t]$ and that the sequence $\{u_n : n \geq 0\}$, with $u_0 \in \mathbb{Z}$ and $u_{n+1} = f(u_n)$ for all $n \geq 0$, is periodic. If p is the smallest period then $p = 1$ or 2.*

Proof. We have $u_{n+p} = u_n$ for all $n \geq 0$. One knows that $x - y$ divides $f(x) - f(y)$ for any integers x, y; in particular that $u_{n+1} - u_n$ divides $f(u_{n+1}) - f(u_n) = u_{n+2} - u_{n+1}$. Therefore $u_1 - u_0$ divides $u_2 - u_1$, which divides $u_3 - u_2$, ... , which divides $u_p - u_{p-1}$, which divides $u_{p+1} - u_p = u_1 - u_0$. That is, we have a sequence of integers that all divide one another and so must all be equal in absolute value. If they are all 0 then $p = 1$. If not then they cannot all be equal, say to $d \neq 0$, else $0 = (u_1 - u_0) + (u_2 - u_1) + (u_3 - u_2) + \cdots + (u_p - u_{p-1}) = pd$. Therefore two consecutive terms must have opposite signs, yet have the same absolute value, so that $u_{n+2} - u_{n+1} = -(u_{n+1} - u_n)$ and therefore $u_{n+2} = u_n$. But then applying f, $p - n$ times to both sides, we deduce that $u_2 = u_0$ and therefore $p = 2$.

This allows us to classify all such polynomials f:

Theorem 1.5.3. *Suppose that $f(t) \in \mathbb{Z}[t]$ and that 0 is a preperiodic point for f but is not in the period. The basic possibilities are:*
a) The period has length 1, and either $f(t) = u$ with $0 \to u \to u \to \ldots$, or $f(t) = (2/u)t^2 - u$ where $u = 1$ or 2, with $0 \to -u \to u \to u \to \ldots$; or
b) The period has length 2, and either $f(t) = 1 + ut - t^2$ with $0 \to 1 \to u \to 1 \to \ldots$, or $f(t) = 1 + t + t^2 - t^3$ with $0 \to 1 \to 2 \to -1 \to 2 \to \ldots$.

Other examples arise by replacing $f(t)$ by $-f(-t)$, or adding a polynomial multiple of $\prod_{i=1}^{k}(t - a_i)$ where the a_i are the distinct integers in the orbit of 0.

Proof by **Exercises**
1.5a. Let $f(t) \in \mathbb{Z}[t]$, and assume that f has a period of length 1, say $f(u) = u$. Then
a) f must be of the form $f(t) = u + (t - u)g(t)$ for some $g(t) \in \mathbb{Z}[t]$.

b) If $f(v) = u$ with $v \neq u$ then $f(t) = u + (t - u)(t - v)g(t)$ for some $g(t) \in \mathbb{Z}[t]$.

c) If $f(w) = v$ then $v - w = w - u = \pm 1$ or ± 2, equals δ say and $g(t) = 2/\delta + (t - w)h(t)$ for some $h(t) \in \mathbb{Z}[t]$.

d) If $f(x) = w$ then $(x - u)(x - v)$ divides $(w - u)$, which is impossible.

1.5b. Assume $f(t) \in \mathbb{Z}[t]$, and f has a period of length 2, say $f(u) = v$ and $f(v) = u$. Then
a) f must be of the form $f(t) = v + u - t + (t - u)(t - v)g(t)$ for some $g(t) \in \mathbb{Z}[t]$.

b) If $f(w) = v$ then $w - v = \pm 1$, so that $g(t) = w - v + (t - w)h(t)$ for some $h(t) \in \mathbb{Z}[t]$.

c) If $f(x) = w$ then $x - u = \pm 1$. If $x - u = w - v = \delta$ then $2 = (x - v)(w - v + (x - w)h(x))$; this implies that $x - v = \delta, 2\delta, -\delta$ or -2δ each of which can be ruled. If $x - u = -(w - v)$ then u, x, w, v are consecutive integers (in this order), and $h(t) = -1 + (t - x)j(t)$ for some $j(t) \in \mathbb{Z}[t]$.

d) Show that if $f(y) = x$ then $y - u$ divides $|x - v| = 2$, and $y - v$ divides $|x - u| = 1$, which is impossible.

1.5c. a) Deduce the cases of the theorem by setting $x = 0$, then $w = 0$ and then $v = 0$.

b) This section was motivated by examples of the first case in the theorem, that is, $f(u) = u + t(t-u)$. An example in the second cases is given by $f(t) = t^2 - 2$, so that $0 \to -2 \to 2 \to 2 \to \ldots$: Start with $x_0 = 4$ and then let $x_{n+1} = f(x_n)$ for all $n \geq 0$. Note that 2 divides each x_n but never 4, so a minor modification of our argument above works to prove that there are infinitely many primes. This sequence has appeared in the literature for another reason: Lucas showed that the Mersenne number $2^n - 1$ is prime if and only if it divides x_{n-2}.

1.5d. Going back to the proof of Proposition 1.5.2, now suppose that $f(x) \in A[x]$ where A is the ring of integers of some number field, and that $u_0 \to u_1 \to \ldots \to u_{p-1} \to u_0$ where p is prime, and $u_0 \in A$.
a) Prove that each $u_j \in A$.
b) Show that $(u_{i+m} - u_i)/(u_m - u_0)$ is a unit of the field for all i and all $m, 1 \leq m \leq p-1$.

We have considered iterations of the map $n \to f(n)$ where $f(t) \in \mathbb{Z}[t]$. If one allows $f(t) \in \mathbb{Q}[t]$ then it is an open question as to the possible period lengths in the integers. Even the simplest imaginable case, $f(x) = x^2 + c$, with $c \in \mathbb{Q}$, is not only open but leads to the magnificent world of dynamical systems (see []). It would certainly be interesting to know what primes divide the numerators when iterating, starting from a given integer.

1.6. Formulas for primes.
i) Let $p_1 = 2 < p_2 = 3 < \ldots$ be the sequence of primes and define $\alpha = \sum_{m \geq 1} p_m / 10^{m^2} = .200300005000000700000001 1 \ldots$. Then $p_m = [10^{m^2}\alpha] - 10^{2m-1}[10^{(m-1)^2}\alpha]$.

Is such a magical number α truly interesting? If one could easily describe α (other than by the definition that we gave) then it might provide an easy way to determine the primes. But with its artificial definition it does not seem like it can be used in any practical way. At first one might suppose that, useful or not, α is quite unique; however the following exercise shows that this is not so.

Exercise 1.6a. Show that there are uncountably many numbers α of this type!

An even less practical formula for primes is derived as follows:
ii) Wilson's theorem tells us that n is a prime if and only if n divides $(n-1)! + 1$. We deduce that $\left[\cos\left(2\pi\left(\frac{(n-1)!+1}{n}\right)\right)\right]$ is equal to either 1 or 0 depending on whether n is prime or not. Summing this over all integers up to x we have an exact formula for the number of primes up to x.

There are surely other ways to identify primes of even less value! Our focus in section ** will be to discuss ways of rapidly determining whether a number is prime.

iii) By 1970, researchers on Hilbert's tenth problem, knew that there exist polynomials f in many variables, such that the positive values taken by f when each variable is set to be an integer, is precisely the set of primes. In 1971 Matijasevič indicated how to construct such a polynomial, and one can construct such polynomials for the set of Fibonacci numbers, for the set of Fermat primes, for the set of Mersenne primes and the set of even perfect numbers, and indeed any *diophantine* set. One can find many different polynomials for the primes, we will give one below with 104 variables of degree 25, and it is known that one

can cut the degree to as low as 5 though for an astronomical cost in terms of the number of variables. No one knows the minimum possible degree, or the minimum possible number of variables.

We will reduce the 104 variables to 26, by only allowing our variables to take non-negative integer values (and so are the sum of four squares of integers): Our polynomial is $k+2$ times

$$\begin{aligned}&1-(n+l+v-y)^2-(2n+p+q+z-e)^2-(wz+h+j-q)^2-(ai+k+1-l-i)^2\\&-((gk+2g+k+1)(h+j)+h-z)^2-(z+pl(a-p)+t(2ap-p^2-1)-pm)^2\\&-(p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m)^2-((a^2-1)l^2+1-m^2)^2\\&-(q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x)^2-((a^2-1)y^2+1-x^2)^2\\&-(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2-(e^3(e+2)(a+1)^2+1-o^2)^2\\&-(16r^2y^4(a^2-1)+1-u^2)^2-(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2)^2.\end{aligned}$$

Stare at this for a while and try to figure out how it works: The key is to determine when does it take positive values, noting that the displayed quantity is equal to 1 minus a sum of squares. Understanding much beyond this seems difficult, and it seems that the only way to appreciate this polynomial is to understand its derivation – see [JSW]. In the current state of knowledge it seems that this absolutely extraordinary and beautiful polynomial is entirely useless in helping us better understand the distribution of primes!

1.7. Special types of primes.

In section 1.2 we asked whether there are infinitely many primes of the form 2^n+1, or of the form 2^n-1, both of which are open questions. One can generalize this by asking whether there are infinitely many primes of the form $k\cdot 2^n\pm 1$ or of the form $k\pm 2^n$ for given integer k. At first sight this seems like a much more difficult question but Erdős showed, ingeniously, how these questions can be resolved for certain integers k:

Let $b_n=2^{2^n}+1$ be the Fermat numbers (remember that b_0,b_1,b_2,b_3,b_4 are prime and $b_5=641\times 6700417$), and let k be any positive integer such that $k\equiv 1 \pmod{641b_0b_1b_2b_3b_4}$ and $k\equiv -1 \pmod{6700417}$. Now

- if $n\equiv 1 \pmod 2$ then $k\cdot 2^n+1\equiv 1\cdot 2^1+1=b_0\equiv 0 \pmod{b_0}$;
- if $n\equiv 2 \pmod 4$ then $k\cdot 2^n+1\equiv 1\cdot 2^2+1=b_1\equiv 0 \pmod{b_1}$;
- if $n\equiv 4 \pmod 8$ then $k\cdot 2^n+1\equiv 1\cdot 2^{2^2}+1=b_2\equiv 0 \pmod{b_2}$;
- if $n\equiv 8 \pmod{16}$ then $k\cdot 2^n+1\equiv 1\cdot 2^{2^3}+1=b_3\equiv 0 \pmod{b_3}$;
- if $n\equiv 16 \pmod{32}$ then $k\cdot 2^n+1\equiv 1\cdot 2^{2^4}+1=b_4\equiv 0 \pmod{b_4}$;
- if $n\equiv 32 \pmod{64}$ then $k\cdot 2^n+1\equiv 1\cdot 2^{2^5}+1=b_5\equiv 0 \pmod{641}$; and
- if $n\equiv 0 \pmod{64}$ then $k\cdot 2^n+1\equiv -1\cdot 2^0+1=0 \pmod{6700417}$.

Every integer n belongs to one of these arithmetic progressions (these are called a *covering system* of congruences), and so we have exhibited a prime factor of $k\cdot 2^n+1$ for every integer n. Therefore we have shown that for a positive proportion of integers k, there is no prime p such that $(p-1)/k$ is a power of 2.

Exercise 1.7a.a) Deduce that $k\cdot 2^n+1$ is composite for every integer $n\geq 0$ (with k as defined above).

b) Prove that $2^n + k$ is composite for every integer $n \geq 0$. (Hence, you have shown that there is no prime p for which $p = k$ is a power of 2.)

c) Let ℓ be any positive integer for which $\ell \equiv -k \pmod{b_6 - 2}$. Prove that $\ell \cdot 2^n - 1$ and $|2^n - \ell|$ is composite for every integer $n \geq 0$

1.7b. (Open question) John Selfridge found the smallest k known for which $k \cdot 2^n + 1$ is always composite: At least one of the primes $3, 5, 7, 13, 19, 37$, and 73 divides $78557 \cdot 2^n + 1$. Is this the smallest such k?

1.7c. Let ℓ be any integer for which $\ell \equiv 1 \pmod{641 b_0 b_2 b_3 b_4}$ and $\equiv 2^{2^3} \pmod{6700417}$, so that $k = \ell^4 \equiv 1 \pmod{641 b_0 b_2 b_3 b_4}$ and is $\equiv 2^{2^5} \equiv -1 \pmod{6700417}$. If $n \equiv 2 \pmod 4$ then, writing $n = 4m + 2$ we have $k \cdot 2^n + 1 = 4(\ell 2^m)^4 + 1$ and the polynomial $4t^4 + 1 = (2t^2 + 2t + 1)(2t^2 - 2t + 1)$. Prove that $k \cdot 2^n + 1$ is composite for every integer $n \geq 0$.

This last exercise shows that we can have $k \cdot 2^n + 1$ composite for all n for reasons other than having a covering system.

Are there infinitely many primes p for which p^2 divides $2^p - 2$? Calculations have been done up to 10^{10} yet the only such primes that have been found are 1093 and 3511. One can ask similar questions about $3^p - 3$, etc.