Algebra in the real world
Hendrik Lenstra
PCMI, July 21, 2022
Lecture notes by Samuel Tiersma

> *In the early days, my business friends would ask me, "How does it feel to be in the real world?" I would say, and I still feel, that mathematics seems much more real to me than business—in the sense that, well, what's the reality in a McDonald's stand? It's here today and gone tomorrow. Now, the integers—that's reality. When you prove a theorem, you've really done something that has a substance to it, to which no business venture can compare for reality.* (Jim Simons, The emissary, June 1998)

The title of my lecture is intended to convey that what Americans call *abstract algebra* is in fact very concrete. It tells us not only that the integers—and that is reality!—have certain properties that we care about, but also *why* they have those properties. I was, as a student, first vividly struck by this power of algebra when I learnt of their application to Fermat numbers and Mersenne numbers: invoking basic results about groups, rings and fields one after the other, one obtains astonishingly efficient and elegant methods for deciding whether a number of the form $2^m \pm 1$ is a prime number. The details are in my lecture. Ever since, I have been using algebra as a means towards understanding the world I live in: the real world of mathematics that is here today and that will not be gone tomorrow.

1 Fermat primes

A *Fermat prime*, named after Pierre de Fermat (1607–1665), is a prime number of the shape $2^m + 1$ with $m \in \mathbb{Z}_{>0}$. Examples: 3, 5, 17, 257, 65537. Historically, these have been of interest in cyclotomy.

Theorem 1.1 (Carl Friedrich Gauss (1777–1855); Pierre Wantzel (1814–1848)). *A regular n-gon is constructible with compass and straightedge if and only if n equals a 2-power (including $2^0 = 1$) times a product of finitely many pairwise distinct Fermat primes (including the empty product 1).* □

It is not difficult to see that $2^m + 1$, with $m > 0$, can only be prime if $m = 2^k$ for some $k \in \mathbb{Z}_{\geq 0}$, so we will restrict our attention to exponents m that are a power of 2. We define for $k \in \mathbb{Z}_{\geq 0}$ the kth *Fermat number* to be $F_k = 2^{2^k} + 1$. It is conjectured that the only Fermat numbers F_k that are prime are the five mentioned above.

Conjecture 1.2. *F_k is prime $\iff$ $k \in \{0, 1, 2, 3, 4\}$.*

It is known that F_k is *not* prime for $5 \leq k \leq 32$, and for a handful of larger k, such as $k = 18\,233954$; for all but two of all these values of k, a *factor* of F_k is known, such as $641 \mid F_5$ (Euler; see Exercise 1.8). The two exceptions are $k = 20$ and $k = 24$. So how can we nonetheless be sure that $F_{20} = 2^{2^{20}} + 1$ and $F_{24} = 2^{2^{24}} + 1$ are not prime? After all, performing trial division up to $\sqrt{F_{20}} = 2.59... \times 10^{157826}$ is out of the question.

Theorem 1.3 (Théophile Pépin (1826–1904; 1877)). *Let $m \in \mathbb{Z}_{\geq 2}$ and $n = 2^m + 1$. Define $r_i \in \mathbb{Z}/n\mathbb{Z}$ for $i \geq 0$ by $r_0 = (3 \bmod n)$, $r_{i+1} = r_i^2$ (again $\bmod\ n$). Then it holds that*

$$n \text{ is prime} \iff r_{m-1} = -1\,(= 2^m).$$

This involves only m ($\approx \frac{\log n}{\log 2}$) arithmetic operations, nowhere near as much as $\sqrt{n}$.

Example. Let $m = 8$, so $n = 257$. Then $r_0 = 3$, $r_1 = 9$, $r_2 = 81$, $r_3 = 6561 = 1421 = -121$, $r_4 = 14641 = 1791 = -8$, $r_5 = 64 = 2^6$, $r_6 = 2^{12} = -2^4$, $r_7 = 2^8 = -1$, so n is prime.

Proof. We start by noting that $r_i = (3^{2^i} \bmod n)$ for all $i \geq 0$.

Case m is odd. Then $3 \mid n$ and $n > 3$, so n is not prime. On the other hand, $3 \mid r_i$ for all i, so $r_{m-1} \not\equiv (-1 \bmod n)$. Thus both assertions are false and the equivalence holds.

Henceforth assume m is even.

$\Longleftarrow$: Suppose $r_{m-1} = -1$. Let $d > 1$ be a divisor of n; showing that $d = n$ will prove the primality of n. Now $3^{2^{m-1}}$ is congruent to -1 modulo n, hence also modulo d. So $3^{2^{m-1}} \not\equiv 1 \bmod d$ but $3^{2^m} \equiv 1 \bmod d$. Hence the order of $(3 \bmod d)$ in the unit group $(\mathbb{Z}/d\mathbb{Z})^*$ divides 2^m but not 2^{m-1}, so equals 2^m. Since the order of an element of a group is at most the order of the group, we have $2^m \leq \#(\mathbb{Z}/d\mathbb{Z})^* \leq d - 1$, whence $d \geq 2^m + 1 = n$. We conclude that $d = n$, as desired.

The converse is slightly more work, some of which is left to the reader in the form of the following exercise.

Exercise 1.4. Suppose A is a finite abelian group with precisely one element of order 2, say ϵ. Then $\#A$ is even, and for each $\alpha \in A$ it holds that $\alpha^{(\#A)/2} \neq \epsilon \iff \alpha^{(\#A)/2} = 1 \iff \exists \beta \in A : \alpha = \beta^2$.

$\Longrightarrow$: Assume n is prime. Then $\mathbb{Z}/n\mathbb{Z}$ is a field with n elements, and we denote it by $\mathbb{F}_n$. In the exercise we take $A = \mathbb{F}_n^*$, of order $n-1 = 2^m$. If $\epsilon \in A$ has order 2, then $(\epsilon-1)(\epsilon+1) = \epsilon^2 - 1 = 0$. Since $\epsilon - 1 \neq 0$ has an inverse in the field $\mathbb{F}_n$, it follows that $\epsilon = -1$, whence A satisfies the hypothesis of the exercise. Taking $\alpha = 3$, we find that $3^{2^{m-1}} \equiv -1 \bmod n$ unless and only unless 3 is a square in $\mathbb{F}_n$.

Suppose there is a $\sqrt{3}$ (i.e. an element whose square is 3) in $\mathbb{F}_n$. There is also a $\sqrt{-1}$, namely $2^{m/2}$, so a $\sqrt{-3}$ exists as well, namely $\sqrt{3} \cdot \sqrt{-1}$. We claim that $\zeta = \frac{-1+\sqrt{-3}}{2}$ has order 3 in $\mathbb{F}_n^*$. Indeed, ζ satisfies $(2\zeta+1)^2 = -3$, so $4(\zeta^2+\zeta+1) = 0$. As 2 has an inverse modulo n, this gives $\zeta^2 + \zeta + 1 = 0$; thus $\zeta^3 = 1$ while $\zeta \neq 1$, proving our claim. Now Lagrange's Theorem—one of the first theorems one encounters in a course on group theory—states: the order of an element of a finite group divides the order of a group. This gives that $3 = \text{order}(\zeta) \mid \#\mathbb{F}_n^* = n - 1 = 2^m$, a contradiction which completes the proof. □

Exercise 1.5. Suppose $p > 2$ is prime and $\alpha \in \mathbb{F}_p^*$. Prove: $\mathbb{F}_p$ has a $\sqrt{\alpha} \iff \alpha^{(p-1)/2} = 1$.

Exercise 1.6. Suppose $p > 3$ is prime. Then $\mathbb{F}_p$ has a $\sqrt{-3} \iff 3 \mid p-1$. Also, $\mathbb{F}_p$ has a $\sqrt{-1} \iff 4 \mid p-1$. Conclude: $\mathbb{F}_p$ has a $\sqrt{3} \iff p \equiv \pm 1 \bmod 12$.

Exercise 1.7. Suppose p is a prime number dividing $F_k = 2^{2^k} + 1$.
(a) If $k \geq 0$, prove that $p \equiv 1 \bmod 2^{k+1}$. [Hint: $2^{2^k} \equiv -1 \bmod F_k$.]
(b) If $k \geq 2$, prove that $p \equiv 1 \bmod 2^{k+2}$. [Hint: $F_{k-1}^{2^{k+1}} \equiv -1 \bmod F_k$.]

Exercise 1.8. **(a)** Using the equalities $641 = 2^7 \cdot 5 + 1 = 5^4 + 2^4$, prove that $2^{32} \equiv -1 \bmod 641$. Deduce that 641 is a prime divisor of $F_5 = 2^{2^5} + 1$.

(b) Using the equalities $431 = 2^4 \cdot 3^3 - 1 = 2^9 - 3^4$ give a similar proof of the primality of 431.

Exercise 1.9. **(a)** Replace in the first 32 rows of the Pascal triangle each even integer by a 0 and each odd integer by a 1. Show this yields the binary expansions of the first 32 odd n for which a regular n-gon is constructible (including $n = 1$).

(b) Show that the only n for which regular n-, $(n+1)$- and $(n+2)$-gons are all constructible with ruler and compass are $n = 1, 2, 3, 5, 255, 65535$.

2 Mersenne primes

A *Mersenne prime* (named after Marin Mersenne, 1588–1648) is a prime number of the shape $2^m - 1$ with $m \in \mathbb{Z}_{\geq 2}$. For example $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$, and

$$2^{2^{2^{2^2-1}-1}-1} - 1 = 170\,141183\,460469\,231731\,687303\,715884\,105727.$$

Historically these have attracted interest due to their connection with perfect numbers. A *perfect number* is a positive integer n that equals the sum of its divisors $< n$ (e.g. $6 = 1+2+3$, $28 = 1+2+4+7+14$ and $496 = 1+2+4+8+16+31+62+124+248$).

Theorem 2.1 (Euclid, $\Longleftarrow$, 3rd century BC; Leonhard Euler (1707–1783), $\Longrightarrow$, 1841)**.** *Let $n \in \mathbb{Z}_{>0}$ be even. Then:*
n is perfect $\iff$ there exists $m \in \mathbb{Z}_{\geq 2}$ such that $2^m - 1$ is prime and $n = 2^{m-1}(2^m - 1)$. □

Conjecturally, *odd* perfect numbers do not exist.

We leave as an exercise to show: if $2^m - 1$ is prime, then m is prime. The converse does not hold, e.g. $2^{11} - 1 = 2047 = 23 \cdot 89$.

It is conjectured that there are infinitely many Mersenne primes. Usually the largest known prime is a Mersenne prime, owing to the Lucas–Lehmer test to be discussed momentarily. As of June 30th, 2022 we know 51 Mersenne primes, and the largest known prime number is $2^{82\,589933} - 1$.

Theorem 2.2 (Lucas–Lehmer test; Édouard Lucas (1842–1891; 1878); Derrick Henry Lehmer (1905–1991; 1930))**.** *Let $m \in \mathbb{Z}_{>2}$ and put $n = 2^m - 1$. Define $s_i \in \mathbb{Z}/n\mathbb{Z}$ ($i \geq 1$) by $s_1 = (4 \bmod n)$ and $s_{i+1} = s_i^2 - 2$ for $i \geq 1$. Then*

$$n \text{ is prime} \iff s_{m-1} = 0.$$

Exercise 2.3. Let s_i ($i \geq 1$) be defined as in the Lucas–Lehmer test, but with $\mathbb{R}$ replacing $\mathbb{Z}/n\mathbb{Z}$. Then for all $i \geq 1$,

$$s_i = (2+\sqrt{3})^{2^{i-1}} + (2-\sqrt{3})^{2^{i-1}}.$$

Proof of Theorem 2.2. In the present proof, the case that m is even is the easy one, and we leave it to the reader. Therefore we assume m is odd. Before beginning the proof proper, we will establish a multiplicative interpretation for $s_{m-1} = 0$. We use a variant of the formula just given, but replacing $2+\sqrt{3}$ by $(\sqrt{2} \cdot \frac{1+\sqrt{3}}{2})^2$. Although this complicates the bases, it simplifies both exponents to be just 2^i. Further, since we want to perform arithmetic not inside $\mathbb{R}$ but modulo n and its divisors, we work with a suitable ring R having an adequate supply of special elements.

Let R be a commutative ring $\neq 0$ with a $\sqrt{2}$, a $\sqrt{3}$ and a $\frac{1}{2}$. Define $\alpha, \beta \in R$ by $\alpha = \frac{\sqrt{2}(1+\sqrt{3})}{2}$ and $\beta = \frac{\sqrt{2}(1-\sqrt{3})}{2}$, so that $\alpha^2 = 2+\sqrt{3}$ and $\beta^2 = 2-\sqrt{3}$. Define $s_i \in R$ ($i \geq 0$) by $s_i = \alpha^{2^i} + \beta^{2^i}$ (as before, $s_1 = 4$ and $s_{i+1} = s_i^2 - 2$ for $i \geq 1$). Because $\alpha\beta = -1$ and 2^{m-1} is even, we arrive at the promised multiplicative interpretation:

$$s_{m-1} = 0 \iff \alpha^{2^{m-1}} = -\beta^{2^{m-1}} = -\alpha^{-2^{m-1}} \iff \alpha^{2^m} = -1 \Longrightarrow \text{order}(\alpha \in R^*) = 2^{m+1}$$

(note that $-1 \neq 1$ in R, since otherwise $0 = 2 \in R^*$, forcing $R = 0$, which we excluded).

The next step is to produce a suitable ring R. Take a divisor $d > 1$ of $n = 2^m - 1$. The ring $\mathbb{Z}/d\mathbb{Z}$ already has a $\frac{1}{2}$, since n is odd. It also has a $\sqrt{2} = 2^{(m+1)/2}$, with indeed square $(\sqrt{2})^2 = 2^{m+1} = 2 \cdot 2^m = 2$; here we used that $d \mid 2^m - 1$, equivalently $2^m \equiv 1 \bmod d$. However,

$\mathbb{Z}/d\mathbb{Z}$ may not have a $\sqrt{3}$ (see Exercise 2.5). Therefore we *adjoin* to $\mathbb{Z}/d\mathbb{Z}$ a $\sqrt{3}$, yielding an *extension ring*

$$R = (\mathbb{Z}/d\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z}) \cdot \sqrt{3} = \{a + b\sqrt{3} : a, b \in \mathbb{Z}/d\mathbb{Z}\}$$

with componentwise addition, and multiplication for which $\sqrt{3} \cdot \sqrt{3} = 3$. Then R is a commutative ring $\neq 0$ having all required special elements, so we can start the actual proof of the asserted equivalence.

$\Longleftarrow$: Assume that $s_{m-1} = 0$ in $\mathbb{Z}/n\mathbb{Z}$, then also in $\mathbb{Z}/d\mathbb{Z}$, hence in R. Therefore our multiplicative interpretation shows

$$n < 2(n+1) = 2^{m+1} = \text{order}(\alpha \in R^*) \leq \#R = d^2,$$

so $d > \sqrt{n}$. But if each divisor of n greater than 1 is greater than $\sqrt{n}$, then n is prime.

$\Longrightarrow$: Suppose n is prime, then necessarily $d = n$. Now $\mathbb{Z}/n\mathbb{Z}$ is a field we denoted $\mathbb{F}_n$, and we contend that $R = \mathbb{F}_n \oplus \mathbb{F}_n\sqrt{3}$ is also a field. Namely, let $a + b\sqrt{3} \in R$ be nonzero, so $a \neq 0$ or $b \neq 0$. Note that $(a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$. If $a^2 - 3b^2 = 0$ then $b \neq 0$, so $\frac{a}{b} = \sqrt{3}$. However, since $n = 2^m - 1 \equiv 1 \bmod 3$ and $n \equiv -1 \bmod 4$, Exercise 1.6 tells us that $\mathbb{F}_n$ does not have a $\sqrt{3}$. So $a^2 - 3b^2 \neq 0$ and, $\mathbb{F}_n$ being a field, it follows that $a + b\sqrt{3} \in R^*$, as contended.

Thus R is a finite field with n^2 elements, denoted $\mathbb{F}_{n^2}$, a *quadratic* extension of $\mathbb{F}_n$. We can now finish off the proof by invoking an elegant theorem from the theory of finite fields.

Theorem 2.4. *Let p be a prime, and $k \in \mathbb{Z}_{\geq 1}$. Let $\mathbb{F}_{p^k}$ be a finite field with p^k elements. Then the automorphism group of $\mathbb{F}_{p^k}$ is cyclic of order k, generated by the* Frobenius automorphism Frob *given by* $\text{Frob}(r) = r^p$ *for all $r \in \mathbb{F}_{p^k}$.*

On the other hand, we know that $R = \mathbb{F}_{n^2}$ has a *conjugation* automorphism $a + b\sqrt{3} \mapsto a - b\sqrt{3}$ of order 2, interchanging α and β. By the theorem this automorphism coincides with Frob, i.e. it sends every $r \in R$ to r^n. In particular, $\alpha^n = \text{Frob}(\alpha) = \beta = -\alpha^{-1}$, whence $\alpha^{2^m} = \alpha^{n+1} = -1$. Thus, our multiplicative interpretation implies $s_{m-1} = 0$. □

This proof illustrates that problems about "ordinary" integers are often most easily solved by working in "extensions". Above we encountered the extensions $\mathbb{F}_n \subset \mathbb{F}_{n^2}$ and $\mathbb{Z}/d\mathbb{Z} \subset R$; for many other problems one uses extensions with base ring $\mathbb{Z}$ or $\mathbb{Q}$, which form the domain of *algebraic number theory.*

Exercise 2.5. Let $m \geq 3$ and $n = 2^m - 1$. Show that n is divisible by a prime $p \equiv \pm 5 \bmod 12$ and that for at least half of all divisors d of n, the ring $\mathbb{Z}/d\mathbb{Z}$ does *not* have a $\sqrt{3}$.