PART I COSMOS MATHEMATICS:
FRACTIONS AND INTEGERS MODULO PRIMES

MICHAEL D. FRIED

1. Warmup with a famous formula of De Moivre

We will combine some algebra and geometry to consider how encryption works. This is supposed to illustrate that you can’t guess beforehand what kind of mathematics will be useful. To warm up, we develop a formula useful in many places in high school mathematics.

Recall the two basic functions of trigonometry: \( \sin(x) \) and \( \cos(x) \). Let \( n \) be a positive integer. The formula I want is for a polynomial of degree \( n \), \( T_n^*(x) \), with this property:

\[ T_n^*(\cos(x)) = \cos(nx). \]

We will use the imaginary number \( i = \sqrt{-1} \). Multiply the following expression formally: \( (\cos(t) + i\sin(t))(\cos(t) - i\sin(t)) \). Why is the result 1 for any value of \( t \)? (Hint: Use that \( \cos(t)^2 + \sin(t)^2 = 1 \).) We also use a formula from trigonometry that has the following memorable form:

\[ (\cos(t_1) + i\sin(t_1))(\cos(t_2) + i\sin(t_2)) = \cos(t_1 + t_2) + i\sin(t_1 + t_2). \]

Write \( x^n + 1/x^n - (x + 1/x)^n \) (using the binomial theorem) as \( U_{n-1}(x + 1/x) \) with \( U_{n-1} \) a polynomial of degree \( n - 1 \). Use an induction to show there is a polynomial \( T_n \) with

\[ T_n(x + 1/x) = x^n + 1/x^n. \]

Plug in \( x = \cos(t) + i\sin(t) \) in (1.2) and apply \( \cos(t)^n + i\sin(t)^n = \cos(nx) + i\sin(nx) \) from an induction using (1.1). The result is

\[ T_n(2\cos(x)) = 2\cos(nx). \]

We call the polynomial \( T_n \) the \( n \)th Chebychev polynomial.

2. Long division

Let \( n \) be an integer not divisible by 2 or 5. Then, \( 1/n \) has a decimal expansion and it is a pure repeating decimal. What does your hand held calculation say is the period — length of the repeating part — of \( 1/23 \)?

2.1. Investigating the periods of \( 1/n \). The period \( n \) has something to do with the powers of 10: Divide \( n \) successively into \( 10^0, 10^1, 10^2, \ldots \), and let the remainders be \( r_0, r_1, r_2, \ldots \). The period is the smallest integer \( k > 0 \) with \( r_k = 1 \). These remainders are all integers with no primes in common with \( n \). We use the symbols \( a|b \) to mean that the integer \( a \) divides the integer \( b \): In the long division of \( a \) into \( b \), there is no remainder.

We now use the definition of prime that appears in Principle 2.2 to see that \( 23|10^{22} - 1 \). Then, we develop from it a very famous formula due to Fermat around 1550, called Fermat’s Little Theorem.

Start with all the numbers between 1 and 22, \( N_{23,1} = \{1, 2, \ldots, 22\} \). Multiply each of them by 10 to get the set \( N_{23,10} = \{10, 10 \cdot 2, \ldots, 10 \cdot 22\} \). Now suppose \( a, b \in N_{23,1} \). Use Princ. 2.2 to see that 23 does not divide \( 10 \cdot a - 10 \cdot b \) unless \( a = b \). So, for every \( a \in N_{23,1} \), there exists a unique \( r_a \in N_{23,10} \) so that \( a - r_a = q_a \cdot 23 \) for some integer \( q_a \).
Big conclusion: $22! - 10^{22}22! = m \cdot 23$ for some integer $m$. Since 23 doesn’t divide $22!$, by Princ. 2.2, 23 does divide $10^{22} - 1$. The same argument allows us to change 23 to any integer $n$, and 10 to any integer $a$ relatively prime to $n$: no prime divides both $a$ and $n$.

2.2. Euler’s $\varphi$-function. The function $\varphi(n)$ counts the integers $m$ between 1 and $n$ that have no primes in common with $n$. We say 10 has order (or period) $k$ modulo $n$ if the length of the repeating part of the fraction $\frac{a}{n}$ is $k$. The next statement tells us why the period of $\frac{a}{n}$ divides $\varphi(n)$. It is the case where $a = 10$. The mathematical phrase $(a, n) = 1$ means that no primes that divide $a$ also divide $n$.

**Proposition 2.1** (Fermat’s Little Theorem). If $(a, n) = 1$, then $n|a^{\varphi(n)} - 1$. We write this as $a^{\varphi(n)} \equiv 1 \bmod n$. This gives an $x \in \mathbb{Z}$ with $ax \equiv 1 \bmod n$ (take $x = a^{\varphi(n)-1}$).

Suppose neither 2 nor 5 divide $n$. Then, the order of 10 modulo $n$ divides $\varphi(n)$. So, the period of $\frac{1}{n}$ divides $\varphi(n)$.

**Proof.** The proof above works by replacing $N_{23,1}$ by the $\varphi(n)$ integers $N_{n,1}$ that are between 1 and $n-1$ and are prime to $n$. Then, replace $N_{23,10}$ by $N_{n,a}$. This gives $a^{\varphi(n)} \equiv 1 \bmod n$.

Suppose $k$ is the smallest integer with $a^k \equiv 1 \bmod n$. Here is why $k|\varphi(n)$. By the Euclidean Algorithm there are integers $u$ and $v$ with this property: $uk + v\varphi(n)$ is $d$, the greatest common divisor of $k$ and $\varphi(n)$. Notice that $v$ and $k$ can have no common prime divisor, or else $d$ would be larger than the greatest common divisor of $k$ and $\varphi(n)$. Check: Using that $a^k \equiv 1 \bmod n$ and $a^{\varphi(n)} \equiv 1 \bmod n$,

$$a^{uk + v\varphi(n)} \equiv (a^k)^u (a^{\varphi(n)})^v \equiv 1 \bmod n.$$ 

That means $d$ must be $k$ and $k = uk + v\varphi(n)$, and so $k|\varphi(n)$.

Let $r_k$ be the reminder from dividing $n$ into $10^k$. The period of the fraction $\frac{1}{n}$ is the smallest integer $k > 1$ with this property. For some integer $k_0 \geq 0$, $r_{k_0+k} = r_k$. So,

$$n|(10^{k_0+k} - 10^{k_0}) = 10^{k_0}(10^k - 1).$$

By the prime principle, no prime of $n$ divides $10^{k_0}$. Conclude that $n$ divides $10^k - 1$, and $k$ is the smallest integer for which this holds, and this is the period of $\frac{1}{n}$.

2.3. Basic Notation. The integers: $\mathbb{Z}$, the nonnegative integers $\mathbb{N}$, the positive integers $\mathbb{N}^+$, the real numbers $\mathbb{R}$, and if $S$ is any set,

$$S^m = \{(s_1, \ldots, s_m) \mid s_i \in S, \ i = 1, \ldots, m\}.$$

- Polynomials over the integers: $\mathbb{Z}[x]$.
- $p_1, p_2, \ldots, p_k$, a listing of the primes in order.
- $a \equiv b \mod n$ if and only if $n|a - b$.

2.4. FTA and Primes. Principle 2.2 has the defining property of a prime $p$. As a corollary of it, there is one and only way to write a positive integer as a product of prime powers.

**Principle 2.2** (Fundamental Theorem of Arithmetic). An integer $p$ is a prime if and only if the following holds for every two integers $a$ and $b$ (see the proof of Cor. 2.5). If $p|a \cdot b$ ($p$ divides $a \cdot b$), then $p|a$ or $p|b$. This shows there is one and only one way to write every positive integer as a product of prime powers.

**Question 2.3.** Consider the number $p = 4$ and the integers $a = 8$ and $b = 2$. How does Principle 2.2 support or disallow that $p = 4$ is a prime in this case?
Let \( p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_n \) the \( n \)th prime. FTa says, any positive \( n \) has a unique expression: \( p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k} \) for some integers \( s_1, s_2, \ldots, s_k \).

Example: \( 15 = 3 \cdot 5 = 2^03^15^17^01^10^1 \cdots \). This notation gives a handy way to write \( n \cdot m \), \( \gcd(n, m) \) and \( \text{lcm}(n, m) \).

2.4.1. *Casting out 9’s, 11’s and 7’s.* Writing an integer \( n \) to the base 10 means writing it as \( a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k 10^k \) with \( 0 \leq a_i \leq 9 \). You can use this to check if \( 9 \mid n \) (if and only if \( 9 \mid a_0 + a_1 + a_2 + \cdots + a_k \)) or \( 11 \mid n \) (if and only if \( 9 \mid a_0 - a_1 + a_2 + \cdots + (-1)^k \cdot a_k \)). Follow these hints for a check of divisibility by 7.

(2.1a) With \( k \cdot 10 + k_0 = n \), notice \( 3k + k_0 + 4 \cdot (k - 2k_0) = 7 \cdot (k - 7k_0) \).

(2.1b) Show 7 divides \( n \) if and only if it divides \( k - 2 \cdot k_0 \).

2.4.2. *Euclidean Algorithm.* Suppose \( n \) and \( m \) are integers. How can we calculate the smallest positive integer \( d \) you can write as \( nu + mv \) with \( u \) and \( v \) any integers? The Euclidean algorithm (EA) shows this is exactly the largest integer dividing both \( n \) and \( m \).

**Example 2.4.** What is the greatest common integer in \( 12121 = r_1 \) and \( 16027 = r_2 \)? What does it have to do with the following process? \( 12121 \mid 16027 \mid (r_1 + r_0) \) to get quotient \( q_1 \) and remainder \( r_2 \). Then, compute \( r_2 \mid r_1 \) to get quotient \( q_2 \) and remainder \( r_3 \); compute \( r_3 \mid r_2 \) to get quotient \( q_3 \) and remainder \( r_4 \).

**Corollary 2.5** (Proof of the Prime Principle). Suppose \( p \) is a prime and \( p \mid a \cdot b \). Suppose \( p \) does not divide \( a \). We apply the EA to find integers \( u, v \) so that \( pu + av = 1 \), or \( b = pbu + abv \). Conclude that \( p \mid b \).

### 3. Using congruences of integers

If \( f \in \mathbb{Z}[x] \) is any polynomial with integer coefficients then, \( a \equiv b \mod m \) implies \( f(a) \equiv f(b) \mod m \).

(3.1a) \( ax \equiv ay \mod m \) if and only if \( x \equiv y \mod m/(a, m) \).

(3.1b) \( x \equiv y \mod m_i, i = 1, \ldots, t \) if and only if \( x \equiv y \mod [m_1, \ldots, m_t] \).

Think of \( x \mod m \) as a set of integers. For example, \( 2 \mod 3 \) is the set
\[ \tilde{2} = \{2 + 3\cdot\mathbb{Z}, 2 + 2\cdot3\cdot\mathbb{Z}, \ldots, 2 + k\cdot3\cdot\mathbb{Z}, \ldots, 2 - 3\cdot2\cdot3\cdot\mathbb{Z}, \ldots, 2 - k\cdot3\cdot\mathbb{Z} \} \].

Then, \( 2 \equiv 5 \mod 3 \) means the sets \( \tilde{2} \) and \( \tilde{5} \) are equal.

3.1. \( \mathbb{Z}/n \) and \( (\mathbb{Z}/n)^* \): **Two abelian groups.** You can add and you can multiply congruences. If \( a \) is an integer modulo \( n \) with \( (a, n) = 1 \), the multiplicative order of \( a \mod n \) is the smallest power of \( a \equiv 1 \mod n \). So, the period of \( \frac{1}{n} \) is the same as the order of 10 mod \( n \). We consider these points.

(3.2a) Euler’s Theorem: If \( p \) is a prime, then for some \( a \) the order of \( a \) is \( p - 1 \).

(3.2b) The order of \( a \mod n \) is the period of \( \frac{1}{a} \) expressed in the base \( a \).

(3.2c) The order of 10 modulo a prime \( p \) varies with \( p \).

There are many unsolved problems about why and how the period of 10 changes as \( n \) changes. Notice that the period of 10 comes up in computing fractions because we do decimals to the base 10. Computer science uses base 2, and base 8 (octal) and base 16 (hexadecimal), rather than base 10. For these different bases, the period of repetition for \( \frac{1}{n} \) would be different.

**Problem 3.1** (A variant on base 10). Suppose \( n \) is odd. How would you phrase the period of \( \frac{1}{n} \) to base 16 so the answer would be similar to the expression in Prop. 2.1 for base 10?
Problem 3.2 (Unsolved). So, possible periods for \( p \) are \( p - 1 \), or \( (p - 1)/2 \). Do these hold for infinitely many primes \( p \)?

3.2. Minimal degree of a polynomial whose values are all divisible by \( m \). Consider the polynomial \( f_m(x) = (x + 1)(x + 2) \cdots (x + m) \).

(3.3a) It has leading coefficient relatively prime to \( m \).

(3.3b) For every integer \( k \), \( m \) divides \( f_m(k) \).

3.3. A special problem using congruences. Let \( Y_m \) be all polynomials \( f \) satisfying (3.3a) and (3.3b).

(3.4a) Suppose \( p \) is a prime. Find the smallest possible degree of a polynomial in \( Y_p \) that satisfies properties (3.3a) and (3.3b) with \( m = p \).

(3.4b) Now do the same for \( m = p^2 \). Hint: Guess at the right answer. Then, if \( f \) satisfies (3.3b) (even if (3.3a) doesn’t hold) so does \( f(x + 1) - f(x) \).

(3.4c) Do as for part (3.4a) with \( m = 1,000,000 \).

(3.4d) Find the function \( F \) where \( F(m) \) is the minimal possible degree of a polynomial in \( Y_m \) for each \( m \).

4. Quadratic equations

The easiest quadratic congruence is \( x^2 \equiv 1 \mod m \). How many solutions does this have under these conditions?

(4.1a) \( m = p \) is a prime.

(4.1b) \( m = p^s \) is a prime power.

(4.1c) \( m = \prod_{i=1}^{\infty} p_i^{e_i} \), an integer presented by the FTA.

Notice that if \( x^2 \equiv y^2 \mod m \), then \( m \mid (x - y)(x + y) \).

4.1. To solve (4.1c) use the Chinese Remainder Theorem. Suppose \( a_1 \) and \( a_2 \) are any integers and \( m_1 \) and \( m_2 \) have no common divisor. Then, the equations \( x \equiv a_i \mod m_i, i = 1,2 \) have some common solution \( x \in \mathbb{Z} \). We call these CRT equations.

4.2. Finding the Solution. Let \( m = m_1m_2 \). Find an \( x_i \) satisfying these simultaneous equations:

(4.2) \( x \equiv 1 \mod m_i \) and \( x \equiv 0 \mod m_j, j \neq i \).

Get \( x_i \) by multiplying \( m_i/m_i \) by an integer that is its inverse \( \mod m_i \). Then, \( x = a_1x_1 + a_2x_2 \) is a solution to the Chinese Remainder Theorem equations.

Theorem 4.1 (Wilson’s Factorial Theorem). If \( p \) is a prime, then \( (p - 1)! \equiv -1 \mod p \).

Further, \( (p - 1)! \equiv (-1)^{\frac{p-1}{2}} \prod_{a=1}^{\frac{p-1}{2}} a^2 \mod p \). So, \( x^2 \equiv -1 \mod p \) has a solution if and only if \( p \equiv 1 \mod 4 \).

4.3. Some quadratics don’t have solutions modulo \( p \). Suppose \( p \) is a prime. Consider \( x^2 - a \equiv 0 \mod p \). Suppose \( x_0 \) is an integer that gives a solution. Put both sides of the equation \( x_0^2 \equiv a \mod p \) to the power \( \frac{p-1}{2} \). Conclude from FLT that \( a^{\frac{p-1}{2}} \equiv 1 \mod p \).

Problem 4.2. Why must there be an \( a \) for which \( x^2 - a \equiv 0 \mod p \) has no solution \( \mod p \)? Hint: Modulo \( p \) there are at most \( n \) solutions to the equation \( P(x) \equiv 0 \mod p \) if \( P \) is a polynomial of degree \( n \). In particular, there are at most \( (p - 1)/2 \) solutions to the equation \( x^{\frac{p-1}{2}} - 1 \equiv 0 \mod p \).
4.4. **Fermat’s Sum of Squares Theorem.** This subsection characterizes integers that are sums of squares of integers. There are two results.

(4.3a) If \( p \) is a prime, then \( p = a^2 + b^2 \) for some \( a,b \in \mathbb{Z} \) if and only if \( p = 2 \) or \( p \equiv 1 \mod 4 \).

(4.3b) Write any integer \( n \) as \( 2^e_1 P_{+1}(n)P_{-1}(n) \) with \( P_{+1}(n) \) (resp. \( P_{-1}(n) \)) composed from the primes dividing \( n \) with \( p \equiv 1 \mod 4 \) (resp. \( p \equiv 3 \mod 4 \)).

Then \( n = a^2 + b^2 \) for some \( a,b \in \mathbb{Z} \) if and only if \( P_{-1}(n) \) is a square.

4.4.1. **Show (4.3a) if \( p \equiv 1 \mod 4 \).** Choose \( k \) the unique integer with \( k < \sqrt{p} < k + 1 \). Find \( 1 \leq \alpha \leq p - 1 \) so \( \alpha^2 \equiv -1 \mod p \). Consider

\[
X = \{x + y\alpha \mid x, y \in \mathbb{Z}, 0 \leq x \leq k, 0 \leq y \leq k\}.
\]

So, \( |X| > p \). Apply the box principle. Thus, there are two integers in \( X \) with the same residues modulo \( p \). So, there exists \( x_0, y_0 \in \mathbb{Z} \) with

\[
x_0 = -y_0\alpha \mod p, \quad x_0^2 + y_0^2 < 2p, \quad x_0^2 + y_0^2 \equiv 0 \mod p.
\]

4.4.2. **An identity.** Apply the following to \( 2^e_1 P_{+1}(n) \) to prove Fermat’s Theorem:

\[
(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.
\]

5. **Abelian cryptography**

First we use FLT to understand how to scramble data embedded in \( \mathbb{Z}/p \) using the polynomial \( x^n \) for \( n \) odd and for infinitely many primes \( p \). A polynomial that permutes the elements of \( \mathbb{Z}/p \) for infinitely many \( p \) is called an exceptional polynomial. The polynomials \( x^n \) are the easiest scrambling (or exceptional) polynomials. This will be an application of Dirichlet’s famous theorem on primes in an arithmetic progression.

Then, we show why the Chebychev polynomials \( T_n \) also allow scrambling data in \( \mathbb{Z}/p \) for infinitely many primes \( p \) if \( n \) is not divisible by 2 or 3.

5.1. **Finite fields of order \( p^2 \).** Suppose \( x^2 - a \) has no solution modulo \( p \). Then, in the same way you can form the complex numbers from the real numbers, you can find a quantity \( \alpha \) so that \( \alpha^2 - a = 0 \) mod \( p \) makes sense. We use the notation \( \mathbb{F}_{p^2} \) for the collection of elements \( u + va,\ u, v \in \mathbb{Z}/p \). We notice that every element in \( \mathbb{F}_{p^2} \), except 0, has an inverse: \( \mathbb{F}_{p^2} \) is a field. Because it has \( p^2 \) elements, we call it a finite field of order \( p^2 \). Now assume \( p \) is odd.

**Proposition 5.1** (FLT for \( \mathbb{F}_{p^2} \)). If \( u + va \neq 0 \), then \( (u + va)^{p^2 - 1} \) is 1 mod \( p \). Hint: The same proof as we used for Fermat’s Little Theorem works here.

Suppose \( a' \) is another integer that is not a square mod \( p \).

**Corollary 5.2.** Then, \( x^2 - a' \) has a zero of the form \( u + va \mod p \). So, any quadric equation in the integers mod \( p \) has a solution in \( \mathbb{F}_{p^2} \).

Here is a hint for the proof of the corollary. Show there must be \((p^2 - 1)/2\) nonzero elements of \( \mathbb{F}_{p^2} \) that aren’t squares in \( \mathbb{F}_{p^2} \), and they are the solutions of the equation \( x^{p^2 - 1} \equiv -1 \mod p \), just like we did it in Prop. 4.2. Then, notice that \( p - 1 \) divides \( \frac{p^2 - 1}{2} \), so no element of the integers mod \( p \) is a solution of this.
5.2. **Why the Chebychev polynomials are exceptional.** Suppose \( p \) is a prime for which \( p^2 - 1 \) and \( n \) have no common divisor. We show that if \( u_0, u_1 \in \mathbb{Z}/p \), then \( T_n(u_0) = T_n(u_1) \), then \( u_0 = u_1 \): \( T_n \) is a one-one map. To do this we consider some \( x_0, x_1 \in \mathbb{F}_p^2 \) so that \( x_0 + 1/x_0 = u_0 \) and \( x_1 + 1/x_1 = u_1 \). Now apply formula (1.2):
\[
T_n(x_0 + 1/x_0) = T_n(x_1 + 1/x_1) = x_0^n + 1/x_0^n = x_1^n + 1/x_1^n.
\]
From this conclude that either \( x_0^n = x_1^n \) or \( x_0^n = 1/x_1^n \). Apply FLT for \( \mathbb{F}_p^2 \) to see this implies, either \( x_0 = x_1 \) or \( x_0 = 1/x_1 \) (and therefore \( x_0 + 1/x_0 = u_0 = x_1 + 1/x_1 = u_1 \)). So, \( T_n \) is a scrambling function.

5.3. **Cryptography with Chebychev polynomials.** Here are the ingredients we would need to know to do Cryptography with the Chebychev polynomials.

- **(5.1a)** If \( (n, 6) = 1 \), show there are infinitely many primes for which \( T_n \) is a scrambling function modulo \( p \). Hint: Use Dirichlet’s Theorem on primes in an arithmetic progression.

- **(5.1b)** For a given \( T_n \) that scrambles mod \( p \), find a polynomial that decrypts \( T_n(M) \) where \( M \) is our message written as an integer mod \( p \). Hint: Try \( T_{n'} \) where \( nn' \equiv 1 \mod p^2 - 1 \).

**Conjecture 5.3** (Schur, 1919; Solved 1969). You get all exceptional (scrambling) polynomials by composing cyclic and Chebychev polynomials.