Review of Group Theory
Definitions, Change of Basis, Trace, Spectral Theorem

Steven J. Miller[*]

June 19, 2004

Abstract

In these notes we review basic number theory and group theory, culminating in applications to cryptography and quadratic reciprocity. A good introduction to group theory is [La2]; for congruences and quadratic reciprocity see [Da1, IR]. The guiding principle behind much of this chapter (indeed, much of number theory) is the search for efficient algorithms. Just being able to write down an expression does not mean we can evaluate it in a reasonable amount of time. Thus, while it is often easy to prove a solution exists, doing the computations (as written) are sometimes impractical.

Contents

1 Cryptography **2**

2 Efficient Algorithms **3**
2.1 Exponentiation 3
2.2 Polynomial Evaluation (Horner's Algorithm) 3
2.3 Euclidean Algorithm 4
2.4 Exercises 6

3 Clock Arithmetic: Arithmetic Modulo n **8**

4 Group Theory **9**
4.1 Definition 9
4.2 Lagrange's theorem 10
4.3 Fermat's Little Theorem 11
4.4 Structure of $(\mathbb{Z}/p\mathbb{Z})^*$ 11

5 RSA Revisited **12**

6 Eisenstein's Proof of Quadratic Reciprocity **13**
6.1 Legendre Symbol 13
6.2 Preliminaries 14
6.3 First Stage 15
6.4 Second Stage 16

[*] sjmiller@math.ohio-state.edu

1 Cryptography

Cryptography is the science of encoding information so that only certain specified people can decode it. We describe some common systems. To prove many of the properties of these crypto-systems will lead us to some of the basic concepts and theorems of algebra and group theory.

Consider the following two password systems: in the first, one chooses two large primes (say 200 digits each, p and q). Let $N = pq$, and display the 400 digit number N for everyone to see; the password is any divisor of N. For the second, choose a random 5000 digit number. Which is more secure? While it is harder to correctly guess 5000 digits than 200, there is a danger in the second system: the computer needs to store the password. In the first, there is no code-book to steal. The computer doesn't need to know p or q: it only needs to know how to divide, and it will know the password when it hears it!

There are so many primes that it is not practical to try all 200 digit prime numbers. The Prime Number Theorem (Theorem **??**) states that there are approximately $\frac{x}{\log x}$ primes smaller than x; for $x = 10^{200}$, this leads to an impractically large number of numbers to check. What we have is a process which is easy in one direction (multiplying p and q), but hard in the reverse (knowing N, right now there is no "fast" algorithm to find p and q).

It is trivial to write an algorithm which is guaranteed to factor N: simply test N by all numbers (or all primes) at most $\sqrt{N}$. While this will surely work, this algorithm is so inefficient that it is practically useless.

Exercise 1.1. *There are approximately 10^{80} elementary objects in the universe (photons, quarks, et cetera). Assume each such object is a powerful supercomputer, capable of checking 10^{20} numbers a second. How many years would it take to check all numbers (or all primes) less than $\sqrt{10^{400}}$? What if each object in the universe was a universe in itself, with 10^{80} supercomputers: how many years would it take now?*

One of the most famous cryptography examples is RSA (see [RSA]). Consider two people, say Alice and Bob, who want to communicate in secret. Instead of sending words, they can send numbers that represent words. We can represent the letter a by 01, b by 02, and so on (and we can have numbers represent capital letters, spaces, punctuation marks, and so on). For example, we write 030120 for the word "cat". It is sufficient to find a secure way for Alice to transmit numbers to Bob. Let us say a message is a number M of a fixed number of digits.

Bob chooses two large primes p and q, and two numbers d and e such that $(p-1)(q-1)$ divides $ed-1$; we explain these choices later. Bob then makes publicly available the following information: $N = pq$ and e, but keeps secret p, q and d. It turns out that this allows Alice to send messages to Bob that only Bob can easily decipher. If Alice wants to send the number M to Bob, Alice first calculates M^e, and then sends Bob the remainder after dividing by N; call this number X. Bob then calculates X^d, whose remainder upon dividing by N is the original message M! The proof of this uses modulo (or clock) arithmetic and basic group theory, which we describe below. Afterwards, we return and prove the claim.

Exercise 1.2. *Let $p = 101$, $q = 97$. Let $d = 2807$ and $e = 23$. Show that this method successfully sends "hi" (0809) to Bob. Note that $(0809)^{23}$ is a sixty-six digit number!*

Exercise 1.3. *Use a quadratic polynomial $ax^2 + bx + c$ to design a security system satisfying the following constraints:*

1. *the password is the triple (a, b, c);*
2. *there are 10 people: any three of them can provide (a, b, c), but no two of them can.*

Generalize the construction: consider a polynomial of degree N such that some people "know more" than others (for example, one person can figure out the password with anyone else, another person just needs two people, and so on).

2 Efficient Algorithms

For computational purposes, often having an algorithm to compute a quantity is not enough; we need an algorithm which will compute *quickly*. For example, in Exercise 1.2 we needed to compute a sixty-six digit number! Below we study three standard problems, and show how to either rearrange the operations more efficiently, or give a more efficient algorithm than the obvious candidate.

2.1 Exponentiation

Consider x^n. The obvious way to evaluate involves $n-1$ multiplications. By writing n in base two, we can evaluate x^n in at most $2\log_2 n$ steps.

We are used to writing numbers in base 10, say

$$x \;=\; a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10^1 + a_0, \quad a_i \in \{1,2,3,4,5,6,7,8,9\}. \tag{1}$$

Base two is similar, except each digit is now either 0 or 1. Let k be the largest integer such that $2^k \le x$. Then

$$x \;=\; b_k 2^k + b_{k-1}2^{k-1} + \cdots + b_1 2 + b_0, \quad b_i \in \{0,1\}. \tag{2}$$

It costs k multiplications to evaluate x^{2^i}, $i \le k$. How? Consider $y_0 = x^{2^0}$, $y_1 = y_0 \cdot y_0 = x^{2^0}\cdot x^{2^0} = x^{2^1}$, $y_2 = y_1 \cdot y_1 = x^{2^2}, \dots, y_k = y^{k-1}\cdot y^{k-1} = x^{2^k}$. Then

$$\begin{aligned} x^n &= x^{b_k 2^k + b_{k-1}2^{k-1} + \cdots + b_1 2 + b_0} \\ &= x^{b_k 2^k} \cdot x^{b_{k-1}2^{k-1}} \cdots x^{b_1 2} \cdot x^{b_0} \\ &= \left(x^{2^k}\right)^{b_k} \cdot \left(x^{2^{k-1}}\right)^{b_{k-1}} \cdots \left(x^2\right)^{b_1} \cdot \left(x^1\right)^{b_0} \\ &= y_k^{b_k} \cdot y_{k-1}^{b_{k-1}} \cdots y_1^{b_1} \cdot y_0^{b_0}. \end{aligned} \tag{3}$$

As each $b_i \in \{0,1\}$, we have at most $k+1$ multiplications above (if $b_i = 1$ we have the term y_i in the product, if $b_i = 0$ we don't). Thus, it costs k multiplications to evaluate the x^{2^i} ($i \le k$), and at most another k multiplications to finish calculating x^n. As $k \le \log_2 n$, we see that x^n can be determined in at most $2\log_2 n$ steps. Note, however, that we do need more storage space for this method, as we need to store the values $y_i = x^{2^i}$, $i \le \log_2 n$.

Exercise 2.1. *Show that it is possible to calculate x^n storing only two numbers at any given time (and knowing the base two expansion).*

Exercise 2.2. *Instead of expanding n in base two, expand n in base three. How many calculations are needed to evaluate x^n this way? Why is it preferable to expand in base two rather than any other base?*

Exercise 2.3. *A better measure of computational complexity is not to treat all multiplications and additions equally, but rather to count the number of digit operations. For example, in 271×31 there are 6 multiplications. We then must add 2 three-digit numbers, which involves at most 4 additions (if we need to carry). How many digit operations are required to compute x^n?*

2.2 Polynomial Evaluation (Horner's Algorithm)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. The obvious way to evaluate $f(x)$ is to calculate x^n and multiply by a_n (n multiplications), calculate x^{n-1} and multiply by a_{n-1} ($n-1$ multiplications) and add, et cetera. There are n additions and $\sum_{k=0}^n k$ multiplications, for a total of $n + \frac{n(n+1)}{2}$ operations. Thus, the standard method leads to about $\frac{n^2}{2}$ computations.

Exercise 2.4. *Prove that* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. Hint: *proceed by induction (see Appendix* **??***). In general,* $\sum_{k=0}^{n} k^d = p_{d+1}(n)$*, where* p_{d+1} *is a polynomial of degree* $d+1$ *with leading term* $\frac{n^d}{d+1}$.

Exercise 2.5. *How many operations are required if we use our results on exponentiation?*

Consider the following grouping to evaluate $f(x)$ (Horner's Algorithm):

$$(((a_n x + a_{n-1})x + a_{n-2})\,x + \cdots + a_1)\,x + a_0. \tag{4}$$

For example,

$$7x^4 + 4x^3 - 3x^2 - 11x + 2 = (((7x+4)x-3)\,x - 11)\,x + 2. \tag{5}$$

Evaluating the long way takes 14 steps; Horner's Algorithm takes 8 steps.

Exercise 2.6. *Prove Horner's Algorithm takes at most* $2n$ *steps to evaluate* $a_n x^n + \cdots + a_0$.

2.3 Euclidean Algorithm

Definition 2.7 (Greatest Common Divisor). *Let* $m, n \in \mathbb{N}$. *The greatest common divisor of* m *and* n*, denoted by* $\gcd(m,n)$ *or* (m,n)*, is the largest integer which divides both* m *and* n.

Definition 2.8 (Relatively Prime, Coprime). *If for integers* m *and* n*,* $\gcd(m,n) = 1$*, we say* m *and* n *are relatively prime (or coprime).*

The Euclidean Algorithm is an efficient way to determine the greatest common divisor of x and y. Without loss of generality, assume $1 < x < y$. The obvious way to determine $\gcd(x,y)$ is to divide x and y by all positive integers up to x. This takes at most $2x$ steps; we show a more efficient way, taking at most about $2\log_2 x$ steps.

Let $[z]$ denote the **greatest integer** less than or equal to z. We write

$$y \;=\; \left[\frac{y}{x}\right] \cdot x + r_1, \quad 0 \le r_1 < x. \tag{6}$$

Exercise 2.9. *Prove that* $r_1 \in \{0, 1, \dots, x-1\}$.

Exercise 2.10. *Prove* $\gcd(x,y) = \gcd(r_1, x)$.

We proceed in this manner until r_k equals zero or one. As each execution results in $r_i < r_{i-1}$, we proceed at most x times (although later we prove we need to apply these steps at most about $2\log_2 x$ times).

$$\begin{aligned}
x &= \left[\frac{x}{r_1}\right] \cdot r_1 + r_2, \;\; 0 \le r_2 < r_1 \\
r_1 &= \left[\frac{r_1}{r_2}\right] \cdot r_2 + r_3, \;\; 0 \le r_3 < r_2 \\
r_2 &= \left[\frac{r_2}{r_3}\right] \cdot r_3 + r_4, \;\; 0 \le r_4 < r_3 \\
&\;\vdots \\
r_{k-2} &= \left[\frac{r_{k-2}}{r_{k-1}}\right] \cdot r_{k-1} + r_k, \;\; 0 \le r_k < r_{k-1}.
\end{aligned} \tag{7}$$

Exercise 2.11. *Prove that if* $r_k = 0$*, then* $\gcd(x,y) = r_{k-1}$*, while if* $r_k = 1$*, then* $\gcd(x,y) = 1$.

We now analyze how large k can be. The key observation is the following:

Lemma 2.12. *Consider three adjacent remainders in the expansion: r_{i-1}, r_i and r_{i+1} (where $y = r_{-1}$ and $x = r_0$). Then $\gcd(r_i, r_{i-1}) = \gcd(r_{i+1}, r_i)$, and $r_{i+1} < \frac{r_{i-1}}{2}$.*

Proof. We have the following relation:

$$r_{i-1} \ = \ \left[\frac{r_{i-1}}{r_i}\right] \cdot r_i + r_{i+1}, \ 0 \leq r_{i+1} < r_i. \tag{8}$$

If $r_i \leq \frac{r_{i-1}}{2}$, then as $r_{i+1} < r_i$, we immediately conclude that $r_{i+1} < \frac{r_{i-1}}{2}$. If $r_i > \frac{r_{i-1}}{2}$, then we note that

$$r_{i+1} \ = \ r_{i-1} - \left[\frac{r_{i-1}}{r_i}\right] \cdot r_i. \tag{9}$$

Our assumptions on r_{i-1} and r_i imply that $\left[\frac{r_{i-1}}{r_i}\right] = 1$. Thus $r_{i+1} < \frac{r_{i-1}}{2}$. □

We count how often we apply these steps. Going from $(x, y) = (r_0, r_{-1})$ to (r_1, r_0) costs one application. Every two applications leads to the first entry in the last pair being at most half of the second entry of the first pair. Thus, if k is the largest integer such that $2^k \leq x$, we see we apply Euclid's Algorithm at most $1 + 2k \leq 1 + 2\log_2 x$ times. Each application requires one integer division, where the remainder is the input for the next step. We have proven

Lemma 2.13. *Euclid's Algorithm requires at most $1 + 2\log_2 x$ divisions to find the greatest common divisor of x and y.*

Euclid's Algorithm provides more information than $\gcd(x, y)$. Let us assume that $r_i = \gcd(x, y)$. Thus, the last equation before Euclid's Algorithm terminated was

$$r_{i-2} \ = \ \left[\frac{r_{i-2}}{r_{i-1}}\right] \cdot r_{i-1} + r_i, \ 0 \leq r_i < r_{i-1}. \tag{10}$$

Therefore, we can find integers a_{i-1} and b_{i-2} such that

$$r_i \ = \ a_{i-1} r_{i-1} + b_{i-2} r_{i-2}. \tag{11}$$

We have written r_i as a linear combination of r_{i-2} and r_{i-1}. Looking at the second to last application of Euclid's algorithm, we find that there are integers a'_{i-2} and b'_{i-3} such that

$$r_{i-1} \ = \ a'_{i-2} r_{i-2} + b'_{i-3} r_{i-3}. \tag{12}$$

Substituting for r_{i-1} in the expansion of r_i yields that there are integers a_{i-2} and b_{i-3} such that

$$r_i \ = \ a_{i-2} r_{i-2} + b_{i-3} r_{i-3}. \tag{13}$$

Continuing by induction, and recalling $r_i = \gcd(x, y)$ yields

Lemma 2.14. *There exist integers a and b such that $\gcd(x, y) = ax + by$. Moreover, Euclid's Algorithm gives a* constructive *procedure to find a and b.*

Thus, not only does Euclid's algorithm show a and b exists, it gives an efficient way to find them.

Exercise 2.15. *Find a and b such that $a \cdot 244 + b \cdot 313 = \gcd(244, 313)$.*

Exercise 2.16. *Add details to complete an alternate, non-constructive proof of the existence of a and b with $ax + by = \gcd(x, y)$:*

1. *Let d be the smallest positive value attained by $ax + by$ as we vary $a, b \in \mathbb{Z}$. Such a d exists. Say $d = \alpha x + \beta y$.*
2. *Show $\gcd(x, y)|d$.*
3. *Let $e = Ax + By > 0$. Then $d|e$. Therefore, for any choice of $A, B \in \mathbb{Z}$, $d|(Ax + By)$.*
4. *Consider $(a, b) = (1, 0)$ or $(0, 1)$, yielding $d|x$ and $d|y$. Therefore $d \leq \gcd(x, y)$. As we've shown $\gcd(x, y)|d$, this completes the proof.*

Note this is a non-constructive proof. By minimizing $ax + by$, we obtain $\gcd(x, y)$, but we have no idea how many steps are required. Prove that a solution will be found either among pairs (a, b) with $a \in \{1, \dots, y-1\}$ and $-b \in \{1, \dots, x-1\}$, or $-a \in \{1, \dots, y-1\}$ and $b \in \{1, \dots, x-1\}$.

Exercise 2.17. *How many steps are required to find the greatest common divisor of $x_1, \dots, x_N$?*

2.4 Exercises

We give some examples and exercises on efficient algorithms / efficient ways to arrange computations. The first assumes some familiarity with calculus, the second with basic combinatorics.

Newton's method: Newton's Method is an algorithm to approximate solutions to $f(x) = 0$ for f a differentiable function on $\mathbb{R}$. Start with x_0 such that $f(x_0)$ is small (we call x_0 the initial guess). Draw the tangent line to the graph of f at x_0, which is given by the equation

$$y - f(x_0) \ = \ f'(x_0) \cdot (x - x_0). \tag{14}$$

Let x_1 be the x-intercept of the tangent line; x_1 is the next guess for the root. Simple algebra gives

$$x_1 \ = \ x_0 - \frac{f(x_0)}{f'(x_0)}. \tag{15}$$

We now iterate, and apply the above procedure to x_1, obtaining

$$x_2 \ = \ x_1 - \frac{f(x_1)}{f'(x_1)}. \tag{16}$$

If we let $g(x) = x - \frac{f(x)}{f'(x)}$, we notice we have the sequence

$$x_0, \ \ g(x_0), \ \ g(g(x_0)), \ \ \dots \tag{17}$$

This sequence will, we hope, converge to the root, at least for x_0 close enough to the root and for f good. How close x_0 has to be is a delicate matter. If there are several roots to f, which root the sequence converges to depends crucially on the initial value x_0 and the function f. In fact its behavior is what is known technically as **chaotic**. Informally, we can say that we have chaos when tiny changes in the initial value give us very palpable changes in the output (see [Dav]).

Exercise 2.18. *Let $f(x) = x^2 - \alpha$, for some $\alpha > 0$. Show Newton's method converges to $\sqrt{\alpha}$, and discuss the rate of convergence (ie, if x_n is accurate to m digits, approximately how accurate is x_{n+1}? (For example, look at $\alpha = 3$ and $x_0 = 2$.) Similarly, investigate $\sqrt[n]{\alpha}$.*

Exercise 2.19. *Modify Newton's Method to find maxima / minima of functions.*

Exercise 2.20. *Let $f(x)$ be a degree n polynomial with complex coefficients. By the Fundamental Theorem of Algebra, there are n (not necessarily distinct) roots. Assume there are m distinct roots. Assign m colors, one to each root. Given a point $x \in C$, we color x with the color of the root that x approaches under Newton's method. Write a computer program to color such sets for some simple polynomials, for example for $x^n - 1 = 0$ for $n = 2, 3$ or 4.*

Combinatorics and Partitions: Assume we have 10 identical cookies and 5 distinct people. How many different ways can we divide the cookies among the people, such that all 10 cookies are distributed? Since the cookies are identical, we cannot tell which cookies a person receives; we can only tell how many. We could enumerate all possibilities (there are 5 ways to have one person receive 10 cookies, 20 ways to have one person receive 9 and another receive 1, and so on). While in principle we can solve the problem, in practice this computation becomes intractable, especially as the number of cookies and people increase.

The number of ways to divide the cookies is $\binom{10+5-1}{5-1}$, where $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ (the number of ways to choose r objects from n objects when order does not matter). In general, if there are C cookies and P people,

Lemma 2.21. *The number of distinct ways to divide C identical cookies among P different people is $\binom{C+P-1}{P-1}$.*

Proof. Consider $C + P - 1$ cookies in a line, and number them 1 to $C + P - 1$. Choose $P - 1$ cookies. There are $\binom{C+P-1}{P-1}$ ways to do this. This divides the cookies into P sets: all the cookies up to the first chosen (which gives the number of cookies the first person receives), all the cookies between the first chosen and the second chosen (which gives the number of cookies the second person receives), and so on. This divides C cookies among P people. Note different sets of $P - 1$ cookies correspond to different partitions of C cookies among P people, and every such partition can be associated to choosing $P - 1$ cookies as above. □

Remark 2.22. *In the above proof, we do not care* which *cookies a person receives. We introduced the numbers for convenience: now cookies 1 through i_1 (say) are given to person 1, cookies $i_1 + 1$ through i_2 (say) are given to person 2, and so on.*

For example, if we have 10 cookies and 5 people, say we choose cookies 3,4,7, and 13 of the 10+5-1 cookies:

$$\odot \quad \odot \quad \otimes \quad \otimes \quad \odot \quad \odot \quad \otimes \quad \odot \quad \odot \quad \odot \quad \odot \quad \odot \quad \otimes \quad \odot$$

This corresponds to person 1 receiving 2 cookies, person 2 receiving 0, person 3 receiving 2, person 4 receiving 5, and person 5 receiving 1.

The above is an example of a partition problem: we are solving $x_1 + x_2 + x_3 + x_4 + x_5 = 10$, where x_i is the number of cookies person i receives. We may interpret Lemma 2.21 as the number of ways to divide an integer N into k non-negative integers is $\binom{N+k-1}{k-1}$.

Exercise 2.23. *Show*

$$\sum_{n=0}^{N} \binom{n+k-1}{k-1} = \binom{N+1+k-1}{k-1}. \tag{18}$$

One can interpret the above as dividing N cookies among k people, where we do not assume all cookies are distributed.

Later (see Chapter **??**) we describe other partition problems, such as representing a number as a sum of primes or integer powers. For example, the famous Goldbach problem says any even number greater than 2 is the sum of two primes (known to be true for integers up to $6 \cdot 10^{16}$ [Ol]). While to date this problem has resisted solution, we have good heuristics which predict that, not only does a solution exist, but how many solutions there are. Computer searches have verified these predictions for large N of size 10^{10}.

Exercise 2.24 (Crude prediction). *By the Prime Number Theorem, there are $\frac{N}{\log N}$ primes less than N. If we assume all numbers $n \leq N$ are prime with the same likelihood (a crude assumption), predict how many ways there are to write N as a sum of two primes.*

Exercise 2.25. *In partition problems, often there are requirements such as everyone receives at least one cookie. How many ways are there to write N as a sum of k non-negative integers? How many solutions of $x_1 + x_2 + x_3 = 2004$ are there if each x_i is an integer and $x_1 \geq 5$, $x_2 \geq 7$, and $x_3 \geq 1000$?*

3 Clock Arithmetic: Arithmetic Modulo n

Let $\mathbb{Z}$ denote the set of integers, and for $n \in \mathbb{N}$ define $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$. We often read $\mathbb{Z}/n\mathbb{Z}$ as the **integers modulo** n.

Definition 3.1 (Congruence). $x \equiv y \bmod n$ *means* $x - y$ *is an integer multiple of* n*. Equivalently,* x *and* y *have the same remainder when divided by* n.

When there is no danger of confusion, we often drop the suffix mod n, writing instead $x \equiv y$.

Lemma 3.2 (Basic Properties of congruences). *For a fixed $n \in \mathbb{N}$ and a, a', b, b' integers we have*

1. $a \equiv b \bmod n$ *if and only if* $b \equiv a \bmod n$.
2. $a \equiv b \bmod n$ *and* $b \equiv c \bmod n$ *implies* $a \equiv c \bmod n$.
3. $a \equiv a' \bmod n$ *and* $b \equiv b' \bmod n$*, then* $ab \equiv a'b' \bmod n$*. In particular* $a \equiv a' \bmod n$ *implies* $ab \equiv a'b \bmod n$ *for all* b.

Exercise 3.3. *Prove the above relations. If $ab \equiv cb \bmod m$, must $a \equiv c \bmod m$?*

For $x, y \in \mathbb{Z}/n\mathbb{Z}$, we define $x + y$ to be the unique number $z \in \mathbb{Z}/n\mathbb{Z}$ such that $n|(x + y - z)$. In other words, z is the unique number in $\mathbb{Z}/n\mathbb{Z}$ such that $x + y \equiv z \bmod n$. One can show that $\mathbb{Z}/n\mathbb{Z}$ is a finite group under addition; in fact, it is a finite ring. (See §4.1 for the definition of a group).

Exercise 3.4 (Arithmetic Modulo n). *Define multiplication of $x, y \in \mathbb{Z}/n\mathbb{Z}$ by $x \cdot y$ is the unique $z \in \mathbb{Z}/n\mathbb{Z}$ such that $xy \equiv z \bmod n$. We often write xy for $x \cdot y$. Prove that this multiplication is well defined, and that an element x has a multiplicative inverse if and only if $(x, n) = 1$. Conclude that if every non-zero element of $\mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse, then n must be prime.* Hint: *use the Euclidean Algorithm to find the inverses.*

Arithmetic modulo n is often called clock arithmetic. If $n = 12$, we have $\mathbb{Z}/12\mathbb{Z}$. If it is 10 o'clock now, in 5 hours it is 3 o'clock, because $10 + 5 = 15 \equiv 3 \bmod 12$.

Definition 3.5 (Least Common Multiple). *Let $m, n \in N$. The least common multiple of m and n, denoted by lcm(m, n), is the smallest positive integer divisible by both m and n.*

Exercise 3.6. *If $a \equiv b \mod n$ and $a \equiv b \mod m$, then $a \equiv b \bmod$ lcm(m, n).*

Let us solve in $\mathbb{Z}$ the equation $2x + 1 = 2y$. The left hand side is odd, the right hand side is even. Thus, there are no integer solutions. What we did is really arithmetic mod 2 or arithmetic in $\mathbb{Z}/2\mathbb{Z}$.

Consider now $x^2 + y^2 + z^2 = 8n + 7$. This never has a solution. Let us study this equation modulo 8. The right hand side is 7 modulo 8. What are the squares modulo 8? $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 1, 4^2 \equiv 0$, and then the pattern repeats (as modulo 8, k and $(8 - k)$ have the same square). We see there is no way to add three squares and get 7. Thus, there are no solutions to $x^2 + y^2 + z^2 = 8n + 7$.

Remark 3.7 (Advanced: Hasse Principle). *In general, when searching for integer solutions one often tries to solve the equation modulo different primes. If there is no solution for some prime, then there are no integer solutions. Unfortunately, the converse is not true. For example, Selmer showed $3x^3 + 4y^3 + 5z^3 = 0$ is solvable modulo p for all p, but there are no rational solutions. We discuss this in more detail in Chapter* **??***).*

Exercise 3.8 (Divisibility Rules). *Prove a number is divisible by 3 (or 9) if and only if the sum of its digits are divisible by 3 (or 9). Prove a number is divisible by 11 if and only if the alternating sum of its digits is divisible by 11 (for example, 341 yields 3-4+1). Find a rule for divisibility by 7.*

Exercise 3.9 (Chinese Remainder Theorem). *Let m, n be relatively prime positive integers. Prove that for any $a, b \in \mathbb{Z}$ there exists a unique $x \bmod mn$ such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$. Generalize to $m_1, \dots, m_k$ and $a_1, \dots, a_k$.*

4 Group Theory

We introduce enough group theory to prove our assertions about RSA. For more details, see [Art, La2].

4.1 Definition

Definition 4.1 (Group). *A set G equipped with a map $G \times G \to G$ denote by $(x, y) \mapsto xy$ is a group if*

1. *(Identity) $\exists e \in G$ s.t. $\forall g \in G : eg = ge = g$.*
2. *(Associativity) $\forall x, y, z \in G : (xy)z = x(yz)$.*
3. *(Inverse) $\forall x \in G, \exists y \in G$ s.t. $xy = yx = e$.*
4. *(Closure) $\forall x, y \in G$: $xy \in G$.*

We have written the group multiplicatively, $(x, y) \mapsto xy$; if we wrote $(x, y) \mapsto x + y$, we say the group is written additively. We call G a finite group if the set G is finite. If $\forall x, y \in G$, $xy = yx$, we say the group is **abelian** or **commutative**.

Exercise 4.2. *Show $\mathbb{Z}/n\mathbb{Z}$ is an (additive) group.*

Exercise 4.3. *Consider the group of $N \times N$ matrices with real entries and non-zero determinant. Prove this is a group under matrix multiplication, and show this group is not commutative if $N > 1$. Is it a group under matrix addition?*

Exercise 4.4. *Let $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, p-1\}$ where $a \cdot b$ is defined to be $ab \bmod p$. Prove this is a (multiplicative) group if p is prime. More generally, let $(\mathbb{Z}/m\mathbb{Z})^*$ be the subset of $\mathbb{Z}/m\mathbb{Z}$ of numbers relatively prime to m. Show $(\mathbb{Z}/m\mathbb{Z})^*$ is a (multiplicative) group.*

Exercise 4.5 (Euler's ϕ-function (or totient function)). *Let $\phi(n)$ denote the number of elements in $(\mathbb{Z}/n\mathbb{Z})^*$. Prove that for p prime, $\phi(p) = p - 1$ and $\phi(p^k) = p^k - p^{k-1}$. If p and q are distinct primes, prove $\phi(p^j q^k) = \phi(p^j)\phi(q^k)$. If n and m are relatively prime, prove that $\phi(nm) = \phi(n)\phi(m)$. Note $\phi(n)$ is the size of the group $(\mathbb{Z}/n\mathbb{Z})^*$.*

Definition 4.6 (Subgroup). *A subset H of G is a subgroup if H is also a group.*

Our definitions imply any group G has at least two subgroups, itself and the empty set ϕ.

Exercise 4.7. *Prove the following equivalent definition: A subset H of G is a subgroup if for all $x, y \in H$, $xy^{-1} \in H$.*

Exercise 4.8. *Let G be an additive subgroup of $\mathbb{Z}$. Prove there exists an $n \in \mathbb{N}$ such that every element of G is an integral multiple of n.*

4.2 Lagrange's theorem

We prove some basic properties of **finite groups** (groups with finitely many elements).

Definition 4.9 (order). *If G is a finite group, the number of elements of G is the order of G and is denoted by $|G|$. If $x \in G$, the order of x in G, ord(x), is the least positive power m such that $x^m = e$, where $e \in G$ is the identity of the group.*

Exercise 4.10. *Prove that, in a finite group, every element has finite order.* Hint: *use the pigeon-hole principle (see §**??**).*

Theorem 4.11 (Lagrange). *Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$. In particular, taking H to be the subgroup generated by $x \in G$, ord(x) $|$ ord(G).*

We first prove two useful lemmas.

Theorem 4.12 (Cayley). *Let H be a subgroup of G, and let $h \in H$. Then $hH = H$.*

Proof. It suffices to show $hH \subset H$ and $H \subset hH$. By closure, $hH \subset H$. For the other direction, let $h' \in H$. Then $hh^{-1}h' = h'$; as $h^{-1}h' \in H$, every $h' \in H$ is also in hH. □

Lemma 4.13. *Let H be a subgroup of a group G. Then for all $g_i, g_j \in G$ either $g_iH = g_jH$ or the two sets are disjoint.*

Proof. Assume $g_iH \cap g_jH$ is non-empty; we must show they are equal. Let $x = g_ih_1 = g_jh_2$ be in the intersection. Multiplying on the right by $h_1^{-1} \in H$ (which exists because H is a subgroup) gives $g_i = g_jh_2h_1^{-1}$. So $g_iH = g_jh_2h_1^{-1}H$. As $h_2h_1^{-1}H = H$, we obtain $g_iH = g_jH$. □

Definition 4.14 (Coset). *We call a subset gH of G a* coset *(actually, a left coset) of H. In general, gH is not a subgroup.*

We now prove Lagrange's Theorem.

Proof of Lagrange's theorem. We claim

$$G = \bigcup_{g \in G} gH \tag{19}$$

Why is there equality? As $g \in G$ and $H \subset G$, each $gH \subset G$, hence their union is contained in G. Further, as $e \in H$, given $g \in G$, $g \in gH$. Thus, G is a subset of the right side, proving equality.

By Cayley's theorem, two cosets are either identical or disjoint. By choosing a subset of the cosets, we show the union in (19) equals a union of disjoint cosets. There are only finitely many elements in G. As we go through all g in G, if the coset gH equals one of the cosets already chosen, we do not include it; if it is new, we do. Continuing this process, we obtain

$$G = \bigcup_{i=1}^{k} g_iH \tag{20}$$

for some finite k and all cosets are disjoint. If $H = \{e\}$, k is the number of elements of G; in general, however, k will be smaller. Each set g_iH has $|H|$ elements, and no two cosets share an element. Thus, $|G| = k|H|$, proving $|H|$ divides $|G|$. □

4.3 Fermat's Little Theorem

Corollary 4.15 (Fermat's Little Theorem). *For any prime p, if $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \bmod p$.*

Proof. As $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$, the result follows from Lagrange's Theorem. □

Exercise 4.16. *One can reformulate Fermat's Little Theorem as the statement that if p is prime, for all a we have $p|a^p - a$. Give a proof for this formulation that does not use group theory.*

Exercise 4.17. *Prove that if for some a, $a^{n-1} \not\equiv 1 \bmod n$ then n is composite.*

Thus, Fermat's Little Theorem is a fast way to show certain numbers are composite (remember exponentiation is fast!). Unfortunately, it is not the case that $a^{n-1} \equiv 1 \bmod n$ implies n is prime. Such composite numbers are called Carmichael numbers (the first few are 561, 1105, and 1729). More generally, one has

Theorem 4.18 (Euler). *If $\gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$.*

Proof. Let $(a,n) = 1$. By definition, $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. By Lagrange's Theorem the order of $a \in (\mathbb{Z}/n\mathbb{Z})^*$ divides $\phi(n)$, or $a^{\phi(n)} \equiv 1 \bmod n$. □

Remark 4.19. *For our applications to RSA, we only need the case when n is the product of two primes. In this case, consider the set $\{1, \dots, pq\}$. There are pq numbers, q are multiples of p, p are multiples of q, and one is a multiple of both p and q. Thus, the number of numbers in $\{1, \dots, pg\}$ relatively prime to pq is $pq - p - q + 1$ (why?). Note this equals $\phi(p)\phi(q) = (p-1)(q-1)$.*

Exercise 4.20. *Korselt [Kor] proved that a composite number n is a Carmichael number if and only if n is square-free and if a prime $p|n$, then $(p-1)|(n-1)$. Prove that if these two conditions are met, then n is a Carmichael number.*

Research Project 4.21 (Carmichael Numbers). *It is known (see [AGP]) that there are infinitely many Carmichael numbers. One can investigate the spacings between adjacent Carmichael numbers. For example, choose a large X, and look at all Carmichael numbers in $[X, 2X]$, say $c_1, \dots, c_{n+1}$. The average spacing between these numbers is about $\frac{2X-X}{n}$ (they are spread out over an interval of size X, and there are n differences: $c_2 - c_1, \dots, c_{n+1} - c_n$. How are these differences distributed?*

*Often, it is more natural to rescale differences and spacings so that the average spacing is 1 (see §**??**). The advantage of such a renormalization is the results are often scale invariant (ie, unitless quantities).*

4.4 Structure of $(\mathbb{Z}/p\mathbb{Z})^*$

The multiplicative group $(\mathbb{Z}/p/Z)^*$ for p prime has a rich structure which will simplify many presentations later.

Theorem 4.22. *For p prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$. Thus, there is an element $g \in (\mathbb{Z}/p\mathbb{Z})^*$ such that*

$$(\mathbb{Z}/p\mathbb{Z})^* \;=\; \{1, 2, \dots, p-2, p-1\} \;=\; \{g^1, g^2, \dots, g^{p-2}, g^{p-1}\}. \tag{21}$$

We say g is a **generator** of the group. For each x there is a unique integer $k \in \{1, \dots, p-1\}$ such that $x \equiv g^k \bmod p$. We say k is the **index** of x relative to g. For each $x \in (\mathbb{Z}/p\mathbb{Z})^*$, the **order** of x is the smallest positive integer n such that $x^n \equiv 1 \bmod p$. For example, if $p = 7$ we have

$$\{1, 2, 3, 4, 5, 6\} \;=\; \{3^6, 3^2, 3^1, 3^4, 3^5, 3^3\}, \tag{22}$$

which implies 3 is a generator (and the index of 4 relative to 3 is 4, because $4 \equiv 3^4 \bmod 7$). Note 5 is also a generator of this group, so the generator need not be unique.

Sketch of the proof. We constantly use the fact that $(\mathbb{Z}/p\mathbb{Z})^*$ is a commutative group: $xy = yx$. Let $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$ with orders m and n for the exercises below. The proof follows from the following:

Exercise 4.23. *Assume $m = m_1 m_2$, with m_1, m_2 relatively prime. Show x^{m_1} has order m_2.*

Exercise 4.24. *Let ℓ be the least common multiple of m and n (the smallest number divisible by both m and n). Prove there is an element z of order ℓ.* Hint: *use the previous exercise to reduce to the case when m and n are relatively prime by changing x. Look at appropriate powers of xy, using $(xy)^r \equiv x^r y^r \bmod p$.*

Exercise 4.25. *By Lagrange's Theorem, the order of any x divides $p-1$ (the size of the group). From this fact and the previous exercises, show there is some d such that the order of every element divides $d \leq p-1$,* and *there is an element of order d and no elements of larger order.*

The proof is completed by showing $d = p - 1$. The previous exercises imply that every element satisfies the equation $x^d - 1 \equiv 0 \bmod p$. As every element in the group satisfies this, and there are $p-1$ elements in the group, we have a degree d polynomial with $p-1$ roots. We claim this can only occur if $d = p-1$.

Exercise 4.26. *Prove the above claim.* Hint: *show any polynomial (that is not identically zero) of degree d has at most d roots modulo p by long division. Namely, if a is a root of $f(x) \equiv 0 \bmod p$, then the remainder of $\frac{f(x)}{x-a}$ must be zero. We then have $f(x) = (x-a)g(z)$, with $g(x)$ of smaller degree than $f(x)$.*

Therefore, $d = p-1$ and there is some element g of order $p-1$; thus, g's powers generate the group. □

Exercise 4.27. *For $p > 2$, $k > 1$, what is the structure of $(\mathbb{Z}/p^k\mathbb{Z})^*$? If all the prime divisors of m are greater than 2, what is the structure of $(\mathbb{Z}/m\mathbb{Z})^*$? For more on the structure of these groups, see any undergraduate algebra textbook (for example, [Art, La2]).*

5 RSA Revisited

We have developed sufficient machinery to prove why RSA works. Remember Bob chose two primes p and q, and numbers d (for decrypt) and e (for encrypt) such that $de \equiv 1 \bmod \phi(pq)$. He made public $N = pq$ and e (and kept secret the two primes and d). Alice wants to send Bob a number M (smaller than N). She encrypts the message by sending $X \equiv M^e \bmod N$. Bob then decrypts the message by calculating $X^d \bmod N$, which we claimed equals M.

As $X \equiv M^e \bmod N$, there is an integer n such that $X = M^e + nN$. Thus, $X^d = (M^e + nN)^d$, and the last term is clearly of the form $(M^e)^d + n'N$ for some n'. We need only show $(M^e)^d \equiv M \bmod N$. As $ed \equiv 1 \bmod \phi(N)$, there is an m such that $ed = 1 + m\phi(N)$. Therefore

$$(M^e)^d \quad = \quad M^{ed} \;=\; M^{1+m\phi(N)} \;=\; M \cdot M^{m\phi(N)} \;=\; M \cdot (M^{\phi(N)})^m. \tag{23}$$

By Euler's Theorem (Theorem 4.18), $M^{\phi(N)} \equiv 1 \bmod N$, which completes the proof.

Why is RSA secure? Assume a third person (say Charlie) intercepts the encrypted message X. He knows X, N and e, and wants to recover M. Knowing d such that $de \equiv 1 \bmod \phi(N)$ makes decrypting the message trivial: one need only compute $X^d \bmod N$. Thus, Charlie is trying to solve the equation $ed \equiv 1 \bmod \phi(N)$; fortunately for Alice and Bob this equation has two unknowns, d and $\phi(N)$! Right now, there is no known fast way to determine $\phi(N)$. Charlie can of course factor N; once he has the factors, he knows $\phi(N)$ and can find d; however, the fastest factorization algorithms make 400 digit numbers unaccessible (for now).

This should be compared to primality testing, which was only recently shown to be fast ([AgKaSa]). Previous deterministic algorithms to test whether or not a number is prime were known to be fast only if certain (expected) conjectures are true. It was an immense achievement showing that there is a deterministic, efficient algorithm. The paper is very accessible, and worth the read.

Remark 5.1. *Our simple example involved computing a sixty-six digit number, and this was for a small N ($N = 9797$). Using binary expansions to exponentiate, as we need only transmit our message modulo N, we never need to compute anything larger than the product of two four digit numbers.*

Remark 5.2. *See [Bon] for a summary of attempts to break RSA. Certain products of two primes are denoted RSA challenge numbers, and the public is invited to factor them. With the advent of parallel processing, many numbers have succumbed to factorization. See http://www.rsasecurity.com/rsalabs/node.asp?id=2092 for more details.*

Exercise 5.3 (Security Concerns). *In the system described, there is no way for Bob to verify that the message came from Alice! Design a system where Alice makes some information public (and keeps some secret) so that Bob can verify that Alice sent the message.*

Exercise 5.4. *Determining $\phi(N)$ is equivalent to factoring N; there is no computational shortcut to factoring. Clearly, if one knows N, one knows $\phi(N)$. If one knows $\phi(N)$ and N, one can recover the primes p and q. Show that if $K = N + 1 - \phi(N)$, then the two prime factors of N are $(K \pm \sqrt{K^2 - 4N})/2$, and these numbers are in fact integers.*

6 Eisenstein's Proof of Quadratic Reciprocity

We conclude this introduction to basic number theory and group theory by giving a proof of quadratic reciprocity (we follow the beautiful exposition in [LP] of Eisenstein's proof). In §2.4, we described Newton's Method to find square-roots of real numbers. Now, we turn our attention to a finite group analogue: for a prime p, given $a \neq 0$, when is $x^2 \equiv a \bmod p$ solvable? For example, if $p = 5$, then $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, 3, 4\}$. Squaring these numbers gives $\{1, 4, 4, 1\} = \{1, 4\}$. Thus, there are two solutions if $a \in \{1, 4\}$ and no solutions if $a \in \{2, 3\}$. The problem of whether or not a given number is a square is solvable: we can simply enumerate the group $(\mathbb{Z}/p\mathbb{Z})^*$, square each element, and see if a is a square. This takes about p steps; quadratic reciprocity will take about $\log p$ steps. For applications, see §**??**.

6.1 Legendre Symbol

We introduce notation. From now on, p and q will always be distinct odd primes.

Definition 6.1 (Legendre Symbol $\left(\frac{\cdot}{p}\right)$). *The Legendre Symbol $\left(\frac{a}{p}\right)$ is*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a non-zero square mod } p \\ 0 & \text{if } a \equiv 0 \bmod p \\ -1 & \text{otherwise} \end{cases} \tag{24}$$

The Legendre symbol is a function on $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We can extend the Legendre symbol to all integers. We only need to know $a \bmod p$, and we define $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$.

Note a is a square mod p if there exists an $x \in \{0, 1, \dots, p-1\}$ such that $a \equiv x^2 \mod p$.

Definition 6.2 (Quadratic Residue / Non-residue). *For $a \not\equiv 0$, if $x^2 \equiv a \bmod p$ is solvable (not solvable) we say a is a quadratic residue (non-residue).*

Exercise 6.3. *Show the Legendre symbol is multiplicative: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Exercise 6.4 (Euler's Criterion). $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$ *for odd* p. Hint: *if* $(a,p)=1$, $a^{\frac{p-1}{2}}$ *squared is* $a^{p-1} \equiv 1$, *so* $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.

Exercise 6.5. *Show* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ *and* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Lemma 6.6. *For* p *an odd prime, half of the non-zero numbers in* $(\mathbb{Z}/p\mathbb{Z})^*$ *are non-zero squares, half are not.*

Proof. As p is odd, $\frac{p-1}{2} \in \mathbb{N}$. Consider the numbers 1^2, $2^2, \dots, (\frac{p-1}{2})^2$. Assume two numbers a and b are equivalent mod p. Then $a^2 \equiv b^2 \bmod p$, so $(a-b)(a+b) \equiv 0 \bmod p$. Thus, either $a \equiv b \bmod p$ or $a \equiv -b \bmod p$ (in other words, $a \equiv p-b$). For $1 \le a, b \le \frac{p-1}{2}$, we cannot have $a \equiv p - b \bmod p$, implying the $\frac{p-1}{2}$ values above are distinct. As $(p-r)^2 \equiv r^2 \bmod p$, the above list is all of the non-zero squares mod p. Thus, half the non-zero numbers are non-zero squares, half are non-squares. □

Remark 6.7. *By Theorem 4.22,* $(\mathbb{Z}/p\mathbb{Z})^*$ *is a cyclic group with generator* g. *Using the group structure, one can prove the above lemma directly: once one shows there is at least one non-residue, the* g^{2k} *are the quadratic residues and the* g^{2k+1} *are the non-residues.*

Exercise 6.8. *Show for any* $a \not\equiv 0 \bmod p$ *that*

$$\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = \sum_{t=0}^{p-1} \left(\frac{at+b}{p}\right) = 0. \tag{25}$$

Initially the Legendre symbol is defined only when the bottom is prime. We now extend the definition. Let $n = p_1 \cdot p_2 \cdots p_t$ be the product of t distinct odd primes. Then $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_t}\right)$; this is the Jacobi symbol, and has many of the same properties as the Legendre symbol. We will study only the Legendre symbol (see [IR] for more on the Jacobi symbol). Note the Jacobi symbol does *not* say that if a is a square (a quadratic residue) mod n, then a is a square mod p_i for each prime divisor.

The main result (which allows us to calculate the Legendre symbol quickly and efficiently) is the celebrated Law of Quadratic Reciprocity:

Theorem 6.9 ((Generalized) Law of Quadratic Reciprocity). *For* m, n *odd and relatively prime,* $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

Gauss gave eight proofs of this deep result (when m and n are prime). If either p or q are equivalent to $1 \bmod 4$, then one has $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, ie, p is a square root modulo q if and only if q is a square root modulo p. We content ourselves with proving the case with m, n prime.

Exercise 6.10. *Using the (Generalized) Law of Quadratic Reciprocity, Exercise 6.5 and the Euclidean algorithm, show one can determine if* a *is a square modulo* m *in logarithmic time (ie, the number of steps is a universal multiple of* $\log m$*). This incredible efficiency is just one of many important properties of the Legendre and Jacobi symbols.*

6.2 Preliminaries

Our goal is to prove

Theorem 6.11 (Quadratic Reciprocity). *Let* p *and* q *be distinct odd primes. Then*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{26}$$

As p and q are distinct, odd primes, both $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ are ± 1. The difficulty is figuring out which signs are correct, and how the two signs are related. We use Euler's Criterion (Exercise 6.4).

The idea behind Eisenstein's proof is as follows: $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$ is -1 to a power. Further, we only need to determine the power modulo 2. Eisenstein shows many expressions are equivalent, modulo 2, to this power. Eventually, we arrive at an expression which is trivial to calculate modulo 2.

As p and q are distinct primes, the Euclidean algorithm implies that q is invertible modulo p, and p is invertible modulo q.

6.3 First Stage

Consider all even multiples of q by any $a \leq p-1$: $\{2q, 4q, 6q, \dots, (p-1)q\}$. Denote a generic multiple by aq. Recall $[x]$ is the greatest integer less than or equal to x. By integer division,

$$aq = \left[\frac{aq}{p}\right]p + r_a, \quad 0 \leq r_a < p - 1. \tag{27}$$

Thus, r_a is the least non-negative number equivalent to $aq \bmod p$.

The numbers $(-1)^{r_a} r_a$ are equivalent to even numbers in $\{0, \dots, p-1\}$. If r_a is even this is clear; if r_a is odd, then $(-1)^{r_a} r_a \equiv p - r_a \bmod p$, and as p and r_a are odd, this is even.

Lemma 6.12. *If* $(-1)^{r_a} r_a \equiv (-1)^{r_b} r_b$*, then* $a = b$*.*

Proof. We quickly get $\pm r_a \equiv r_b \bmod p$. If the plus sign holds, then $r_a \equiv r_b \bmod p$ implies $qa \equiv qb \bmod p$. As q is invertible mod p, we get $a \equiv b \bmod p$, which yields $a = b$ (as a and b are even integers between 0 and $p-1$).

If the minus sign holds, then $r_a + r_b \equiv 0 \bmod p$, or $qa + qb \equiv 0 \bmod p$. Multiplying by $q^{-1} \bmod p$ now gives $a + b \equiv 0 \bmod p$. As a and b are even integers between 0 and $p-1$, $0 < a + b \leq 2(p-1)$. The only integer strictly between 0 and $2p$ which is equivalent to $0 \bmod p$ is p; however, p is odd and $a + b$ is even. Thus, the minus sign cannot hold, and the elements are all distinct. □

Lemma 6.13.

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{a \text{ even}} r_a}. \tag{28}$$

Proof. For each even a, $qa \equiv r_a \bmod p$. Thus, mod p:

$$\begin{aligned}
\prod_{a \text{ even}} qa &\equiv \prod_{a \text{ even}} r_a \\
q^{\frac{p-1}{2}} \prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} r_a \\
\left(\frac{q}{p}\right) \prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} r_a,
\end{aligned} \tag{29}$$

where the above follows from the fact that we have $\frac{p-1}{2}$ choices for an even a (to get $q^{\frac{p-1}{2}}$) and Euler's Criterion. As a ranges over all even numbers from 0 to $p-1$, so too do the distinct numbers $(-1)^{r_a} r_a \bmod p$. Thus, mod p,

$$\begin{aligned}
\prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} (-1)^{r_a} r_a \\
\prod_{a \text{ even}} a &= (-1)^{\sum_{a \text{ even}} r_a} \prod_{a \text{ even}} r_a.
\end{aligned} \tag{30}$$

Combining gives

$$\left(\frac{q}{p}\right)(-1)^{\sum_{a \text{ even}} r_a} \prod_{a \text{ even}} r_a \equiv \prod_{a \text{ even}} r_a. \tag{31}$$

As each r_a is invertible mod p, so is the product. Thus,

$$\left(\frac{q}{p}\right)(-1)^{\sum_{a \text{ even}} r_a} \equiv 1 \bmod p. \tag{32}$$

As $\left(\frac{q}{p}\right) = \pm 1$, the lemma follows by multiplying both sides by $\left(\frac{q}{p}\right)$. □

Therefore, it is sufficient to determine $\sum_{a \text{ even}} r_a \bmod 2$. We make one last simplification. By integer division, we have

$$\sum_{a \text{ even}} qa = \sum_{a \text{ even}} \left(\left[\frac{qa}{p}\right] p + r_a\right) = \sum_{a \text{ even}} \left[\frac{qa}{p}\right] p + \sum_{a \text{ even}} r_a. \tag{33}$$

As we are summing over even a, the left hand side above is even. Thus, the right hand side is even, so

$$\begin{aligned} \sum_{a \text{ even}} \left[\frac{qa}{p}\right] p &\equiv \sum_{a \text{ even}} r_a \bmod 2 \\ p \sum_{a \text{ even}} \left[\frac{qa}{p}\right] &\equiv \sum_{a \text{ even}} r_a \bmod 2 \\ \sum_{a \text{ even}} \left[\frac{qa}{p}\right] &\equiv \sum_{a \text{ even}} r_a \bmod 2, \end{aligned} \tag{34}$$

where the last line follows from the fact that p is odd, so mod 2, dropping the factor of p from the left hand side doesn't change the parity. We have reduced the proof of quadratic reciprocity to calculating $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$.

6.4 Second Stage

Consider the rectangle with vertices at $A = (0,0)$, $B = (p,0)$, $C = (p,q)$ and $D = (0,q)$. The upward sloping diagonal is given by the equation $y = \frac{q}{p}x$. As p and q are distinct odd primes, there are no pairs of integers (x,y) on the line AC.

We now interpret $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$. Consider the vertical line with x-coordinate a. Then $\left[\frac{qa}{p}\right]$ gives the number of pairs (x,y) with x-coordinate equal to a and y-coordinate an integer at most $\left[\frac{qa}{p}\right]$. Thus, $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$ is the number of integer pairs (in the rectangle $ABCD$) with even x-coordinate that are below the line AC.

We add some non-integer points: $E = (\frac{p}{2}, 0)$, $F = (\frac{p}{2}, \frac{q}{2})$, $G = (0, \frac{q}{2})$ and $H = (\frac{p}{2}, q)$. We prove

Lemma 6.14. *The number of integer pairs under the line AC (inside the rectangle) with even x-coordinate is congruent mod 2 to the number of integer pairs under the line AF.*

Let $a > \frac{p}{2}$ be an even integer. The integer pairs on the line $x = a$ are $(a,0), (a,1), \dots, (a,q)$. There are $q+1$ pairs. As q is odd, there are an even number of integer pairs on the line $x = a$. As there are no integer pairs on the line AC, for a fixed $a > \frac{p}{2}$, mod 2 there are the same number of integer pairs *above* AC as there are *below* AC.

Further, the number of integer pairs *above* AC is equivalent mod 2 to the number of integer pairs below AF on the line $x = p - a$. To see this, consider the map which takes (x,y) to $(p-x, q-y)$. As $a > \frac{p}{2}$ and is even, $p - a < \frac{p}{2}$ and is odd. Further, every odd $a < \frac{p}{2}$ is hit (given $a_{odd} < \frac{p}{2}$, start with the even number $p - a_{odd} > \frac{p}{2}$).

Let $\#FCH_{even}$ be the number of integer pairs (x, y) in triangle FCH with x even.

Let $\#EBCH$ be the number of integer pairs in the rectangle $EBCH$; $\#EBCH \equiv 0 \bmod 2$ (we've shown each vertical line has an even number of pairs).

Let $\#AFE_{even}$ be the number of integer pairs (x, y) in the triangle AFE with x even, and let $\#AFE$ be the number of integer pairs in the triangle AFE.

We need to calculate $\sum_{a \text{ even}} \left[\frac{qa}{p}\right] \bmod 2$:

$$\begin{aligned}\sum_{a \text{ even}} \left[\frac{qa}{p}\right] &= \#AFE_{even} + \#EBCH - \#FCH \\ &\equiv \#AFE_{even} + \#EBCH + \#FCH \\ &= \#AFE_{even} + \#FCH + \#EBCH \\ &= \#AFE + \#EBCH \\ &= \#AFE. \end{aligned} \tag{35}$$

Therefore, $\mu = \sum_{a \text{ even}} \left[\frac{qa}{p}\right] \equiv \#AFE \bmod 2$, and we have

$$\left(\frac{q}{p}\right) = (-1)^{\mu}. \tag{36}$$

Reversing the rolls of p and q, we see that

$$\left(\frac{p}{q}\right) = (-1)^{\nu}, \tag{37}$$

where $\nu \equiv \#AFG \bmod 2$, with $\#AFG$ equal to the number of integer pairs in the triangle AFG.

Now, $\mu + \nu = \#AFE + \#AFG$, which is the number of integer pairs in the rectangle $AEFG$. There are $\frac{p-1}{2}$ choices for x and $\frac{q-1}{2}$ choices for y, giving $\frac{p-1}{2}\frac{q-1}{2}$ pairs of integers in the rectangle $AEFG$. Thus,

$$\begin{aligned}\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) &= (-1)^{\mu+\nu} \\ &= (-1)^{\#AFE + \#AFG} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}, \end{aligned} \tag{38}$$

which completes the proof of Quadratic Reciprocity. □

References

[AgKaSa] M. Agrawal, N. Kayal and N. Saxena, *Primes is in P*, to appear.

[AGP] W. R. Alford, A. Granville, A. and C. Pomerance, *There are Infinitely Many Carmichael Numbers*, Ann. Math. 139, 703-722, 1994.

[Art] M. Artin, *Algebra*, Prentice Hall.

[Bon] D. Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices of the American Mathematical Society, **46**, 2, 1999, 203–213.

[Dav] R. Daveney, *An Introduction to Chaotic Dynamical Systems*, Perseus Books, 2nd edition, 2003.

[Da1] H. Davenport, *The Higher Arithmetic*, Cambridge University Press.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, Graduate Texts in Mathematics 84, 1990.

[Kor] A. Korselt, *Probléme chinois*, L'intermédiaire math. 6, 143-143, 1899.

[La2] S. Lang, *Undergraduate Algebra*, Springer-Verlag, second edition, 1986.

[LP] R. Laubenbacher and D. Pengelley, *Gauss, Eisenstein, and the "third" proof of the quadratic reciprocity theorem: Ein kleines Schauspiel*, Math. Intelligencer 16 (1994), no. 2, 67-72.

[Ol] T. Oliveira e Silva, *Verification of the Goldbach Conjecture Up to* $6 \cdot 10^{16}$, NMBRTHRY@listserv.nodak.edu mailing list, Oct. 3, 2003, http://listserv.nodak.edu/scripts/wa.exe?A2=ind0310&L=nmbrthry&P=168.

[RSA] R. Rivest, A. Shamir, A. and L. Adleman, *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Comm. ACM 21, 120-126, 1978.

Index

ϕ-function, 9

Carmichael numbers, 11
chaotic, 6
clock arithmetic, 8
congruence, 8
coprime, 4
cryptography, 2

Euclidean algorithm, 4
Euler’s criterion, 14
exponentiation, 3

Fermat’s Little Theorem, 11
function
    totient, 9
Fundamental Theorem of Algebra, 7

Goldbach problem, 7
greatest common divisor, 4
greatest integer, 4
group, 9
    abelian, 9
    commutative, 9
    coset, 10
    finite, 10
    generator, 11
    index, 11
    order, 10, 11
    subgroup, 9

Hasse Principle, 9
Horner’s algorithm, 3

Jacobi symbol, 14

Lagrange’s Theorem, 10
least common multiple, 8, 12
Legendre symbol, 13

modulo, 8

Newton’s method, 6

Quadratic Reciprocity, 14

relatively prime, 4
residue
    quadratic, 13
RSA, 2, 12