Intro to Theoretical Crypto
Scribe: Don Sheehy February 13, 2005

1 Basic Notation

We will quickly review the basic notation we will be using. We denote the set of integers by $\mathbb{Z}$ and let $\mathbb{Z}^+$ be the positive integers and $\mathbb{Z}_0^+$ be the nonnegative integers. The set of integers modulo m is denoted $\mathbb{Z}_m$, and we will go into more detail about some of the properties of this set a little later on. The greatest common divisor of a pair of integers, $gcd(a, b)$ will be written as (a, b) according to the standard shorthand.

Given a continued fraction (CF) representation, the partial quotients are denoted $q_0, q_1, \ldots$ and the ith approximation is written

$$\frac{P_i}{Q_i} = q_0 + \frac{1}{q_1+}\ \frac{1}{q_2+}\cdots\frac{1}{q_i}.$$

When we write that an approximation $\frac{P_i}{Q_i}$ is equal to some fraction $\frac{a}{b}$, we actually mean that $P_i = a$ and $Q_i = b$. In this respect we abuse the usual notion of equivalence of fractions but it is worthwhile so that we can reason specifically about the numerator and denominator of the successive approximations.

2 Continued Fractions Revisited

2.1 CF for Rational Numbers

Let's take a look at what happens when we do our continued fraction representation of a rational number.

$$\begin{aligned}
\frac{18}{13} &= 1 + \frac{5}{13} && (1)\\
&= 1 + \frac{1}{2 + \frac{3}{5}} && (2)\\
&= 1 + \frac{1}{2 + \frac{1}{1+\frac{2}{3}}} && (3)\\
&= 1 + \frac{1}{2 + \frac{1}{1+\frac{1}{1+\frac{1}{2}}}} && (4)
\end{aligned}$$

In the notation we have been using in this class we can write this CF as

$$\frac{1}{1} + \frac{1}{2+} \; \frac{1}{1+} \; \frac{1}{1+} \; \frac{1}{2}.$$

Notice that unlike previous examples of using continued fractions for approximating π and the golden ratio, this list of fractions is finite. As we will show, it turns out that this will always be the case when we start with a rational number. Of course, this is exactly what we would hope for when we think about continued fractions as giving better and better rational approximations of a number; the best rational approximation of a rational number is simply that number itself.

Claim 1. *The continued fraction approximation for a rational number $\frac{a}{b}$ will converge to $\frac{P_i}{Q_i} = \frac{a}{b}$ in a finite number of steps.*

Proof. The proof is a straightforward induction on the remainder $a \bmod b$. □

3 Modular Arithmetic

3.1 Notation

For integers, $a, b \in \mathbb{Z}$, and $m \in \mathbb{Z}^+$, we say "a is *congruent* to $b \bmod m$" if and only if m divides the difference $a - b$ with no remainder. The standard notation for congruence (also called *equivalence* mod m) is as follows.

$$a \equiv b \pmod{m}.$$

At times it will be useful to use mod as a binary operation that gives the remainder when a is divided by b. That is, we will define

$a \bmod m =$ the unique integer $b \in \{0, \ldots, m-1\}$ such that $a \equiv b \pmod{m}$.

There is a slight difference in the way mathematicians and computer scientists understand the meaning of modular arithmetic. For example, to the mathematician, $a \bmod m$ is denoted $[a]_m$ and represents the equivalence class of all integers in the arithmetic progression $\{a + km | k \in \mathbb{Z}\}$. To the computer scientist, $a \bmod m$ represents the smallest non-negative integer of the form $a+km$ where $k \in \mathbb{Z}$. These two definitions are very similar and make

very little difference syntactically, but semantically, one is an integer while the other is an infinite class of integers. To reconcile these two different views, we need only observe that the computer scientist view is to simply designate one special element from equivalence class $[a]_m$, specifically the smallest nonnegative one, and use this represent the whole class. In number theory, this set of designated elements, one from each equivalence class, is called a *reduced residue system mod m*. We let $\mathbb{Z}_m$ denote the set $\{0, \ldots, m-1\}$ (the reduced residue system mod m).

3.2 Inverses mod m

Recall the following interesting fact about the relationship between the numerators and denominators of consecutive approximations $\frac{P_i}{Q_i}, \frac{P_{i+1}}{Q_{i+1}}$ for a continued fraction of a rational number $\frac{a}{b}$ with $(a, b) = 1$.

$$P_i Q_{i+1} - P_{i+1} Q_i = \pm 1 \text{ for all } i. \tag{5}$$

What is the significance of this relationship? Recalling the connection between continued fractions and the Extended Euclidean Algorithm, we will see that a will have an inverse mod$m$ exactly when $(a, m) = 1$.

Theorem 2. *If $a, m \in \mathbb{Z}^+$ and $(a, m) = 1$ then a has an inverse a^{-1} in $\mathbb{Z}_m$.*

Proof. Let $\frac{P_i}{Q_i}$ be the ith approximation in the continued fraction for $\frac{a}{m}$. We have seen that for some n, the nth approximation is exact, $\frac{P_n}{Q_n} = \frac{a}{m}$. Recalling the relationship in 5, we get

$$P_{n-1} Q_n - P_n Q_{n-1} = m P_{n-1} - a Q_{n-1} = \pm 1.$$

Thus,

$$a Q_{n-1} \equiv \pm 1 \pmod{m}$$

□

3.3 Other facts to know about $\mathbb{Z}_m$

More formally, we note that $\mathbb{Z}_m$ is a ring. That is, it is a group under the addition operation with identity 0, and it is a semigroup under multiplication with identity 1. So, what keeps $\mathbb{Z}_m$ from being a full-fledged field? The problem lies in the fact that not all elements in $\mathbb{Z}_m$ will have multiplicative

inverses. The preceding section proves that some element $a \in \mathbb{Z}_m$ has an inverse if and only if $(a, m) = 1$; that is, if and only if a and m are relatively prime. So, in order for all elements to have inverses, all elements of $\{0, \ldots, m-1\}$ are relatively prime to m. This is the case if and only if m is prime.

Theorem 3. *For all primes p, $\mathbb{Z}_p = GF(p)$, where $GF(p)$ is the unique finite field with p elements.*

You may recall from Field Theory that all finite fields are of order (size) p^m for some prime p and positive integer m. The finite field $GF(p^m)$ can be viewed as a vector space over $GF(p)$. Because, there exists exactly one finite field of size p^m for each choice of p and m, the preceding theorem states that the unique finite field of prime order p is isomorphic to the integers $\mod p$.

As we have seen in the preceding example, the ring $\mathbb{Z}_m$ is not a field for all m.

4 The Chinese Remainder Theorem

The Chinese Remainder Theorem is a neat application of the preceding theorems of modular arithmetic.

Theorem 4. *Let $m_1, \ldots, m_k$ be pairwise relatively prime integers and let M be their product $\prod_{i=1} km_i$. For all $a \in \mathbb{Z}_M$, there is a unique Chinese Remainder Representation $\langle a_1, \ldots, a_k \rangle$ of a for the given moduli $m_1, \ldots, m_k$. Furthermore, for all $a, b \in Z_M$, it is true that*

$$a + b = \langle a_1 + b_1, \ldots, a_k + b_k \rangle \tag{6}$$
$$a - b = \langle a_1 - b_1, \ldots, a_k - b_k \rangle \tag{7}$$
$$a \times b = \langle a_1 \times b_1, \ldots, a_k \times b_k \rangle \tag{8}$$

Before proceeding to the proof, we pause a moment to go through an example.

Example 1. *Let $m_1 = 3, m_2 = 4, m_3 = 5$.*

Proof of Theorem 4. □

Now that we have proved the theorem, we can be sure as mathematicians that every $a \in \mathbb{Z}_m$ has a unique CRR for a given set of moduli. However, as computer scientists, we want algorithms to go back and forth between the CRR representation to the integer representation. In one direction, this task is quite simple. If we want to compute the CRR given the number a, we simply divide a by each modulus and list the remainders. However, the reverse direction needs a tad more cleverness.

The main idea is that we want a kind of basis of CRR representations that we can sum together to get a as a linear sum with coefficients a_i. That is to say, we want

$$\begin{aligned} I_1 &= \langle 1, 0, 0, \ldots, 0 \rangle \\ I_2 &= \langle 0, 1, 0, \ldots, 0 \rangle \\ \vdots &= \vdots \\ I_k &= \langle 0, 0, \ldots, 0, 1 \rangle, \end{aligned}$$

so that we can write

$$a = \langle a_1, \ldots, a_k \rangle = \left(\sum_{i=1}^{k} a_i I_i \right) \bmod m.$$

We can get close to such a list by observing that the CRR for $\frac{M}{m_i}$ will have 0's for every modulus other than m_i. For example, we can compute these values for the preceding example.

$$\begin{aligned} \frac{M}{m_1} &= 20 = \langle 2, 0, 0 \rangle \\ \frac{M}{m_2} &= 15 = \langle 0, 3, 0 \rangle \\ \frac{M}{m_3} &= 12 = \langle 0, 0, 2 \rangle \end{aligned}$$

Now, we'd like a way to reduce these nonzero entries to 1's and we'll have exactly the basis we wanted. For example we'd like to write the following.

$$a \equiv \frac{1}{2}\frac{M}{m_1}a_1 + \frac{1}{3}\frac{M}{m_2}a_2 + \frac{1}{2}\frac{M}{m_3}a_3 \pmod{m}$$

However, $\frac{1}{2}$ and $\frac{1}{3}$ aren't actually elements of the ring $\mathbb{Z}_m$. Yet, all is not lost. As we have seen, 2 and 3 *do* have multiplicative inverses mod$m$ when $(2, m) = 1$ and $(3, m) = 1$. So, we can use the extended Euclidean algorithm to compute the inverses and complete the computation.

References