Math Circle
November 15, 2009

1 Integers Modulo N

Think of a clock. It has 12 numbers: 1, 2, ..., 12. It will be convenient to associate $12 \leftrightarrow 0$, so that we are focusing on the numbers: $\{0, 1, 2, \ldots, 11\}$. We will denote these 12 numbers as $\mathbb{Z}_{12}$, which are called the *integers modulo twelve*.

We can do arithmetic using these numbers in the familiar way, except that we must "wrap around" when we go to high. For instance, if it is 11 o' clock, and two hours go by, what time is it? This can be expressed as:

$$11 + 2 \equiv 1 (\text{ mod } 12) \tag{1}$$

Here, when we hit 12, we "wrap around" back to zero, so 11+2 goes $11 \stackrel{+1}{\rightarrow} 12{=}0 \stackrel{+1}{\rightarrow} 1$. Notice also that in the regular integers, 11+2=13, and that when 13 is divided by 12, the *remainder* is 1. Indeed, this is how you should think about arithmetic in $\mathbb{Z}_{12}$: perform the arithmetic as usual, and then at the end "reduce modulo 12," that is, find the remainder of your answer when you divide it by 12. Subtraction works the same way. However, if you end up at a negative answer, it is useful to keep adding 12 until you get something between 0 and 11. Imagine it is 1 o' clock. What time was it four hours ago (obviously, it was 9 o' clock)? We can write this as 1-4 = -3. Then to get it between 0 and 11, we add 12, and arrive at 9.

There is nothing special about 12. We could do the same thing modulo N, for N any positive integer. For instance, if $N = 2$, the we are just looking at *bits*, i.e. $\mathbb{Z}_2 = \{0, 1\}$. If you have done boolean logic tables before, then it may be familiar that in $\mathbb{Z}_2$, 1+1=0 (since 1+1 = 2, and the remainder when 2 is divided by 2 is zero).

The integers modulo N obey some very nice properties that we are familiar with from normal integers: Commutativity, Associativity, Distributivity. In addition, one of the nicest properties is the following. First some notation. For any integer x and any modulus N, there is a unique element in $\mathbb{Z}_N$ that "represents" x. Namely, the remainder when x is divided by N. For a random integer x, we will write x when we wish to refer to the integer, and $\bar{x}$ when we are referring to the unique element in $\mathbb{Z}_N$ that represents x (notice that in the notation "$\bar{x}$", the modulus N is implicit, i.e. it is assumed that we are agreed what modulus N we are talking about). Sometimes, $x = \bar{x}$ (when?). The following says that when performing arithmetic in $\mathbb{Z}_N$, it does not matter if you reduce the numbers before or after the computation:

$$\overline{x+y} = \bar{x} + \bar{y}$$
$$\overline{xy} = \bar{x}\bar{y}$$

For example, in $\mathbb{Z}_9$, I can compute 13+4 in two different ways: 1) Add them to get 17, then "reduce modulo 9" to get 8; or 2) First reduce 13 to 4, then add 4+4=8. Sometimes (especially for multiplication), it is easier to reduce *before* computing.

2 Quadratic Residues

An integer $x \in \mathbb{Z}_N$ is a quadratic residue (modulo N) if $\exists y \in \mathbb{Z}_N$ such that $x \equiv y^2 (\text{mod } N)$, i.e. x is a *square* modulo N. The set of quadratic residues in $\mathbb{Z}_N$ is denoted QR_N, and the non-residues are denoted QNR_N.

In Abstract Algebra, they show that $\mathbb{Z}_N$ is fundamentally different if N is a prime verses composite number. It turns out that for our purposes, some of these differences are important. For instance, for prime moduli, we have:

Theorem 2.1. *When multiplying two integers in $\mathbb{Z}_p$ for a prime modulus p:*

$$\begin{array}{lrl} 1) & QR * QR & = QR \\ 2) & QR * QNR & = QNR \\ 3) & QNR * QR & = QNR \\ 4) & QNR * QNR & = QR \end{array}$$

3 Legendre Symbol

The question of whether or not an integer is a *square* in $\mathbb{Z}_N$ is so important, there is a special symbol in math that represents this question. It is called the Legendre Symbol, named after the French mathematician Adrien-Marie Legendre (1752-1833), who, among other things, proved Fermat's last theorem for $n = 5$, and conjectured the prime number theorem and law of quadratic reciprocity (see below). Succinctly, it is written:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \in QR_p \\ -1 & \text{if } a \in QNR_p \end{cases} \tag{2}$$

If $a \notin \mathbb{Z}_p$ (e.g. $a > p$), then first find a's representative $\overline{a}$ in $\mathbb{Z}_p$.

4 Jacobi Symbol

The Jacobi symbol is a generalization of the Legendre symbol to moduli N that are not prime. If $N = p_1^{\alpha_1} \dots p_l^{\alpha_l}$, then the Jacobi Symbol is defined as:

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_l}\right)^{\alpha_l} \tag{3}$$

Properties of Jacobi symbol:

1. $\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right)$
2. $\left(\frac{a^2}{N}\right) = 1$ as long as $gcd(a, N) = 1$
3. $\left(\frac{a}{NM}\right) = \left(\frac{a}{N}\right)\left(\frac{a}{M}\right)$
4. $\left(\frac{a}{N^2}\right) = 1$ as long as $gcd(a, N) = 1$
5. Law of Quadratic Reciprocity:

   a) If a and N are both *odd*, then:
   $$\left(\frac{N}{a}\right) = \left(\frac{a}{N}\right)\left(-1\right)^{\left(\frac{a-1}{2}\right)\left(\frac{N-1}{2}\right)} = \begin{cases} -\left(\frac{a}{N}\right) & \text{if } a, N \equiv 3 (\text{mod } 4) \\ \left(\frac{a}{N}\right) & \text{otherwise} \end{cases}$$
   b) $$\left(\frac{2}{N}\right) = \left(-1\right)^{\left(\frac{n^2-1}{8}\right)} = \begin{cases} 1 & \text{if } N \equiv 1, 7 (\text{mod } 8) \\ -1 & \text{if } N \equiv 3, 5 (\text{mod } 8) \end{cases}$$

6. a) If $\left(\frac{a}{N}\right) = -1$, then $a \in QNR_N$
   b) If $a \in QR_N$, then $\left(\frac{a}{N}\right) = 1$
   c) However, if $\left(\frac{a}{N}\right) = 1$, then we don't know if $a \in QR_N$ or $a \in QNR_N$. Indeed, if $N = pq$ is the product of two primes, and $\mathcal{S}$ is the set of all numbers in $\mathbb{Z}_N$ with Jacobi symbol $+1$, then exactly half the elements of $\mathcal{S}$ are quadratic residues, and exactly half are non-residues (the former have form (QR, QR), while the latter have form (QNR, QNR)).

5 Quadratic Residuosity and Cryptography

In 1982, Shafi Goldwasser and Silvio Micali created a public-key encryption scheme that makes use of many of the properties we have been studying. The encryption scheme is used to encrypt messages one-bit at a time as follows.

Setup. Pick two large primes p and q, and set $N = pq$. Pick a random $u \in QNR_N$ such that u has Jacobi Symbol one. Publish (N, u).

Encryption. Pick a random element $r \in \mathbb{Z}_N$. If you want to encrypt '0', set $E(0) = r^2$. Otherwise, if you want to encrypt '1', set $E(1) = ur^2$

Decryption. Given ciphertext c, use factorization of N to determine if c is a quadratic residue. Output '0' if so, output '1' otherwise.

Note that the security of the scheme follows from the fact that the ciphertext c looks like a random element of $\mathbb{Z}_N$ with Jacobi Symbol $+1$, and by property 6c) above, exactly half of these are quadratic residues and half are non-residues. So if an eavesdropper cannot determine if $c \in QR_N$, then they have at best a 50-50 chance of guessing.

Note also that, as with all modern cryptography, the security of the scheme is based on a hardness assumption, which says that without knowledge of the factorization of N, it is hard to determine if a random element in $\mathbb{Z}_N$ is a quadratic residue or not.