Lecture Notes 10

43 Modular Multiplication

Two integers a and b are *relatively prime* if they have no common prime factors, or equivalently, if $\gcd(a, b) = 1$. Let $\mathbf{Z}_n^* \subseteq \mathbf{Z}_n$ contain those integers that are relatively prime to n, so

$$\mathbf{Z}_n^* = \{a \in \mathbf{Z}_n \mid \gcd(a, n) = 1\}.$$

Define Euler's *totient function* to be the cardinality of $\mathbf{Z}_n^*$:

$$\phi(n) = |\mathbf{Z}_n^*|.$$

Properties of $\phi(n)$:

1. If p is prime, then $\phi(p) = p - 1$.
2. More generally, if p is prime and $k \geq 1$, then $\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$.
3. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

These properties enable one to compute $\phi(n)$ for all $n \geq 1$ provided one knows the factorization of n. For example,

$$\phi(126) = \phi(2)\phi(3^2)\phi(7) = (2-1)(3-1)(3^{2-1})(7-1) = 1 \cdot 2 \cdot 3 \cdot 6 = 36.$$

The 36 elements of $\mathbf{Z}_{126}^*$ are: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 53, 55, 59, 61, 65, 67, 71, 73, 79, 83, 85, 89, 95, 97, 101, 103, 107, 109, 113, 115, 121, 125.

44 Modular Exponentiation and Euler's Theorem

Recall the RSA encryption and decryption functions

$$\begin{aligned} E_e(m) &= m^e \bmod n \\ D_d(c) &= c^d \bmod n \end{aligned}$$

where $n = pq$ is the product of two distinct large primes p and q. We see that both are based on modular exponentiation of large integers, an operation that we now explore in some depth.

In section 42.3, we defined the operation $\otimes$ on all of $\mathbf{Z}_n$. An important fact is that $\mathbf{Z}_n^*$ is closed under $\otimes$, that is, if a and b are both in $\mathbf{Z}_n^*$, then $a \otimes b$ is also in $\mathbf{Z}_n^*$. This follows from the observation that if neither a nor b share a prime factor with n, then neither does their product ab. It can be shown that $\mathbf{Z}_n^*$ is an Abelian group under the operation of $\otimes$. This means that it satisfies the following properties:

Associativity $\otimes$ is an associative binary operation on $\mathbf{Z}_n^*$. In particular, $\mathbf{Z}_n^*$ is closed under $\otimes$.

Identity 1 is an identity element for $\otimes$ in $\mathbf{Z}_n^*$, that is $1 \cdot x = x \cdot 1 = x$ for all $x \in \mathbf{Z}_n^*$.

Inverses For all $x \in \mathbf{Z}_n^*$, there exists another element $x^{-1} \in \mathbf{Z}_n^*$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Commutativity $\otimes$ is commutative. (This is only true for *Abelian* groups.)

Example: Let $n = 26 = 2 \cdot 13$. Then

$$\mathbf{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

and

$$\phi(26) = |\mathbf{Z}_{26}^*| = 12.$$

The inverses of the elements in $\mathbf{Z}_{26}^*$ are given in Table 1. The bottom row of the table gives equiva-

Table 1: Table of inverses in $\mathbf{Z}_{26}^*$.

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25
$=$	1	9	-5	-11	3	-7	7	-3	11	5	-9	-1

lent integers in the range $[-12, \ldots, 13]$. This makes it apparent that $(26 - x)^{-1} = -x^{-1}$. In other words, the last row reads back to front the same as it does from front to back except that all of the signs flip from $+$ to $-$ or $-$ to $+$, so once the inverses for the first six numbers are known, the rest of the table is easily filled in.

It is not obvious from what I have said so far that inverses always exist for members of $\mathbf{Z}_n^*$. The fact that they do will become apparent later when we show how to compute inverses.

Recall Euler's ϕ function which was defined in section 43 to be $|\mathbf{Z}_n^*|$, the cardinality of $\mathbf{Z}_n^*$. From the properties given there, one can derive an explicit formula for $\phi(n)$.

Theorem 1 *Write n in factored form, so $n = p_1^{e_1} \cdots p_k^{e_k}$. where $p_1, \ldots, p_k$ are distinct primes and $e_1, \ldots, e_k$ are positive integers.*[1] *Then*

$$\phi(n) = (p_1 - 1) \cdot p_1^{e_1 - 1} \cdots (p_k - 1) \cdot p_k^{e_k - 1}.$$

When p is prime, we have simply $\phi(p) = (p - 1)$, and for the product of two distinct primes, $\phi(pq) = (p - 1)(q - 1)$. Thus, $\phi(26) = (13 - 1)(2 - 1) = 12$, as we have seen.

A general property of finite groups is that if any element x is repeatedly multiplied by itself, the result is eventually 1. That is, 1 appears in the sequence $x, (x \otimes x), (x \otimes x \otimes x), \ldots$, after which the sequence repeats. For example, for $x = 5$ in $\mathbf{Z}_{26}^*$, we get the sequence $5, 25, 21, 1, 5, 25, 21, 1, \ldots$. The result of multiplying x by itself k times can be written x^k. The smallest integer k for which $x^k = 1$ is called the *order* of x, sometimes written $\mathrm{ord}(x)$. It follows from general properties of groups that the order of any element of a group divides the order of the group. For $\mathbf{Z}_n^*$, we therefore have $\mathrm{ord}(x) \,|\, \phi(n)$. From this fact, we immediately get

Theorem 2 (Euler's theorem) $x^{\phi(n)} \equiv 1 \pmod{n}$ *for all $x \in \mathbf{Z}_n^*$.*

As a special case, we have

Theorem 3 (Fermat's theorem) $x^{(p-1)} \equiv 1 \pmod{p}$ *for all x, $1 \leq x \leq p - 1$, where p is prime.*

Corollary 4 *Let $r \equiv s \pmod{\phi(n)}$. Then $a^r \equiv a^s \pmod{n}$ for all $a \in \mathbf{Z}_n^*$.*

[1] By the fundamental theorem of arithmetic, every integer can be written uniquely in this way up to the ordering of the factors.

Proof: If $r \equiv s \pmod{\phi(n)}$, then $r = s + u\phi(n)$ for some integer u. Then using Euler's theorem, we have

$$a^r \equiv a^{s+u\phi(n)} \equiv a^s \cdot (a^u)^{\phi(n)} \equiv a^s \cdot 1 \equiv a^s \pmod{n},$$

as desired. ■

The importance of this corollary to RSA is that it gives us a condition on e and d that ensures the resulting cryptosystem works. That is, if we require that

$$ed \equiv 1 \pmod{\phi(n)}, \tag{1}$$

then it follows from Corollary 4 that $D_d(E_e(m)) = m^{ed} \equiv m \pmod{n}$ for all messages $m \in \mathbf{Z}_n^*$, so $D_d()$ really does decrypt messages in $\mathbf{Z}_n^*$ that are encrypted by $E_e()$.

What about the case of messages $m \in \mathbf{Z}_n - \mathbf{Z}_n^*$? There are several answers to this question.

1. For such m, either $p \mid m$ or $q \mid m$ (but not both because $m < pq$). If Alice ever sends such a message and Eve is astute enough to compute $\gcd(m, n)$ (which she can easily do), then Eve will succeed in breaking the cryptosystem. So Alice doesn't really want to send such messages if she can avoid it.

2. If Alice sends random messages, her probability of choosing a message not in $\mathbf{Z}_n^*$ is only about $2/\sqrt{n}$. This is because the number of "bad" messages is only $n - \phi(n) = pq - (p-1)(q-1) = p + q - 1$ out of a total of $n = pq$ messages altogether. If p and q are both 512 bits long, then the probability of choosing a bad message is only about $2 \cdot 2^{512}/2^{1024} = 1/2^{511}$. Such a small probability event will likely never occur during the lifetime of the universe.

3. For the purists out there, RSA does in fact work for all $m \in \mathbf{Z}_n$, even though Euler's theorem fails for $m \notin \mathbf{Z}_n^*$. For example, if $m = 0$, it is clear that $(0^e)^d \equiv 0 \pmod{n}$, yet Euler's theorem fails since $0^{\phi(n)} \not\equiv 1 \pmod{n}$. We omit the proof of this curiosity.