Geoffrey Parker - grp352
HW 26: 5.1 - 5.5
M328K
May 1st, 2012

5.1 Theorem. *If p and q are distinct prime numbers and W is a natural number with $(W, pq) = 1$, then $W^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.*

Proof. Let p and q be distinct prime numbers and W be a natural number with $(W, pq) = 1$. Since p and q are prime and $(W, pq) = 1$, $(W, p) = 1$ and $(W, q) = 1$. So by Fermat's Little Theorem $W^{p-1} \equiv 1 \pmod{p}$ and $W^{q-1} \equiv 1 \pmod{q}$. Then by theorem 1.18 $W^{(p-1)(q-1)} \equiv 1^{q-1} \pmod{p}$ and $W^{(p-1)(q-1)} \equiv 1^{p-1} \pmod{q}$. So by theorem 4.21 $W^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. □

5.2 Theorem. *Let p and q be distinct primes, k be a natural number, and W be a natural number less than pq. Then*

$$W^{1+k(p-1)(q-1)} \equiv W \pmod{pq}.$$

Proof. Let p and q be distinct primes, k be a natural number, and W be a natural number less than pq. Consider two cases:

Case 1: $(W, pq) = 1$. In this case, theorem 5.1 states that $W^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. So by theorem 1.18 $W^{k(p-1)(q-1)} \equiv 1^k \pmod{pq}$. And by theorem 1.14 $W^{k(p-1)(q-1)}W \equiv W \pmod{pq}$, or $W^{1+k(p-1)(q-1)} \equiv W \pmod{pq}$.

Case 2: $(W, pq) \neq 1$. In this case, $p \mid W$ or $q \mid w$, but not both, because pq is the smallest natural number that both p and q divide. Without loss of generality, assume that $p \mid W$ and $q \nmid W$. So by theorem 1.6 $p \mid W^{1+k(p-1)(q-1)}$, and by theorem 1.2 $p \mid W^{1+k(p-1)(q-1)} - W$. Then by the definition of conrgruence, we have

$$W^{1+k(p-1)(q-1)} \equiv W \pmod{p}$$

. Now, since q is prime and $q \nmid W$, we know that $(W, q) = 1$. Fermat's Little Theorem then gives us $W^{q-1} \equiv 1 \pmod{q}$, and by theorem 1.18 we can say $W^{k(p-1)(q-1)} \equiv 1^{k(p-q)} \pmod{q}$. Theorem 1.14 says

$$W^{1+k(p-1)(q-1)} \equiv W \pmod{q}$$

. Therefore by theorem 4.21 $W^{1+k(p-1)(q-1)} \equiv W \pmod{pq}$. □

5.3 Theorem. *Let p and q be distinct primes and E be a natural number relatively prime to $(p-1)(q-1)$. Then there exist natural numbers D and y such that*

$$ED = 1 + y(p-1)(q-1).$$

Proof. Let p and q be distinct primes and E be a natural number relatively prime to $(p-1)(q-1)$. By our lemma there exists a D such that $ED \equiv 1 \pmod{(p-1)(q-1)}$. Then by definition of congruence $(p-1)(q-1) \mid ED - 1$, and by definition of divides there exists a natural number y such that $y(p-1)(q-1) = ED - 1$. Therefore there exist natural numbers D and y such that $ED = 1 + y(p-1)(q-1)$. □

Lemma: If n is a natural number and a is an integer coprime with n then there exists a unique natural number b less than n such that $ab \equiv 1 \pmod{n}$.

Proof. Let n be a natural number and a be an integer coprime with n. Let $x_1, x_2, \ldots, x_{\phi(n)}$ be the natural numbers less than n which are coprime with n. Let $S = \{ax_1, ax_2, \ldots, ax_{\phi(n)}\}$. Note that by theorem 4.31 the elements of S are pairwise incongruent. By definition of complete residue systems, each element s_i of S is congruent to some element y_i of the canonical complete residue system modulo n. Since each x is coprime with n and a is coprime with n, by theorem 4.28 s_i is coprime with n. This implies, by theorem 4.29, that y_i is coprime with n. However, the set of x's is defined to contain all natural numbers less than n. Therefore $y_i = x_j$ for some j. Also, for any natural numbers i and j less than $\phi(n)$, if $i \neq j$ then $y_i \not\equiv y_j \pmod{n}$ because if they were congruent modulo n, then s_i and s_j would be too, which we know isn't true. We have now established that each element of S is congruent modulo n to some distinct x. Since $|S| = \phi(n)$ and $x_1 = 1$ there must be exactly one element t of S which is congruent modulo n to 1. And $t = ab$ for some natural number b less than n. Therefore there exists a unique natural number b less than n such that $ab \equiv 1 \pmod{n}$. □

5.4 Theorem. *Let p and q be distinct primes, W be a natural number less than pq, and E, D, and y be natural numbers such that $ED = 1 + y(p-1)(q-1)$. Then*

$$W^{ED} \equiv W \pmod{pq}.$$

Proof. Let p and q be distinct primes, W be a natural number less than pq. Let E, D, and y be natural numbers such that $ED = 1 + y(p-1)(q-1)$. Then by theorm 5.2 [$W^{ED} \equiv W \pmod{pq}$. □

5.5 Exercise. *Consider two distinct primes p and q. Describe every step of the RSA Public Key Coding System. State what numbers you choose to make public, what messages can be encoded, how messages should be encoded, and how messages are decoded. What number should be called the encoding exponent and what number should be called the decoding exponent?*

Solution. First, key generation. Presumably p and q are large random primes, 2048 or 4096 bits, chosen with a good random number generator. Then let $n = pq$. Note that $\phi(n) = (p-1)(q-1)$. Then choose e to be a small number coprime with $\phi(n)$. Typically this is $2^{16}+1$, which is prime. Now we need to find d such that $ed \equiv 1 \pmod{\phi(n)}$. Our lemma above assures us that d exists, so we can rearrange this to give $\phi(n)y = ed - 1$ or $ed - \phi(n)y = 1$. Since e and $\phi(n)$ are known and $(e, \phi(n)) = 1$ we can use the Extended Euclidean Algorithm to find d. The public key will be the pair of numbers e, n and the private key the pair d, n.

Now say that Alice wants to send a message m to Bob over an insecure channel. We are assuming that m is a natural number which is the encoding in some scheme, such as UTF-8, of the actual message Alice wants to send. Alice will then look up Bob's public key, e_B, n_B and use it to encrypt her message. She will create a cyphertext c by calculating $c = m^{e_B} \pmod{n_B}$. Alice then sends this to Bob. Bob, and only Bob, can recover the original message by calculating $c^{d_B} \pmod{n_B} = m^{d_B e_B} \pmod{n_B}$, which theorem 5.4 assures us is equal to m.

RSA can also be used in reverse to ensure authenticity. This is known as signing. Bob can sign a message m by calculating $s = m^{d_B} \pmod{n_B}$. Then anyone can use Bob's public key to recover the original message m by calculating $s^{e_B} \pmod{n_B}$. However, since they are using Bob's public key, they know that the signed message must have been created with Bob's private key, and thus Bob must be the author.

However this is inefficient, as m could be very large. So Bob employs a hash function h. A hash function is a function where the elements of the range are much smaller than the elements of the domain, and it is statistically very unlikely for two given elements of the domian to map to the same element of the range (this is known as a collision). Since hash functions are very effecient to compute, Bob will find $h(m)$, which is much smaller than m and sign that, giving $s = h(m)^{d_B} \pmod{n_B}$. Bob then sends both m and s to Alice. Alice can calulate $h(m)$ with the m she recieves and $x = s^{e_B} \pmod{n_B}$. Alice can then compare $h(m)$ with x. If they match, she knows that Bob was the author of the message.

These two properties can be combined. If Alice has keys e_A, n_A and d_A, n_A, then she can send a secure, authenticated message m to Bob like so. First she hashes the message giving $h(m)$ and calculates $s = h(m)^{d_A} \pmod{n_A}$. Then she concatenates together m, s, and her name into a new message m'. She then encrypts m' with Bob's public key, giving cyphertext $c = m'^{e_B} \pmod{n_B}$. This cyphertext is then sent to Bob. Bob then receives c and recovers $m' = c^{d_B} \pmod{n_B}$. Since m' contains Alices name, he then looks up Alices public key and uses it to authenticate the message. He finds $h(m)$ and $h(m)' = s^{e_A} \pmod{n_A}$ and compares the two to be sure that they are equal. So Bob is the only one who could decrypt the message, and Bob knows that Alice is the only one who could have sent the message, ensuring both secrecy and authentication. □