Algebraic Cryptography
Homework 1

Due Wednesday, 6 September 2017

Problem 1. The *Division Algorithm* states that for nonnegative integers $a, b \in \mathbb{Z}$ with $b \neq 0$ (called the *dividend* and *divisor*, there exist unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < b$ (called the *quotient* and *remainder*) for which $a = qb + r$. Prove the Division Algorithm.

Proof. Consider the set $\{k \in \mathbb{Z}_{\geq 0} \mid a - kb \geq 0\}$. This is nonempty since it contains zero, and it is bounded since any integer larger than a is not in the set. Therefore, this set has a maximal element, which we will call q. Set $r := a - qb$ which is nonnegative by the definition of q. Then notice that $r - b = a - (q+1)b$, which must be negative by the maximality of q. Therefore $r < b$.

To prove uniqueness, suppose that there are integers q', r' with $0 \leq r' < b$ so that $a = q'b + r'$. Then $|r - r'| < b$, and $r - r' = (q' - q)b$, thus $|q' - q|\, b < b$ and hence $|q' - q| < 1$. Therefore $|q' - q| = 0$, so $q = q'$ and so also $r = r'$. ■

Problem 2. The *greatest common divisor* of two nonzero integers a, b is the largest positive integer which divides both a, b. We denote this $\gcd(a, b)$. A linear combination of a, b over $\mathbb{Z}$ is a quantity of the form $ax + by$ where $a, b \in \mathbb{Z}$. *Bezout's identity* asserts that the greatest common divisor of a, b is the smallest positive linear combination of a, b over $\mathbb{Z}$. Symbolically,

$$\gcd(a, b) = \min\{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}.$$

Prove Bezout's identity.

Proof. First, we note that any common divisor c of a, b also divides any linear combination of a, b. Indeed, in this case $a = cm$ and $b = cn$ for some integers m, n. Thus for any integers x, y, we have

$$ax + by = (cm)x + (cn)y = c(mx + ny),$$

and therefore c divides this linear combination.

Second, we let $d = ax + by$ be the *smallest* positive linear combination of a, b. We will show that d divides both a, b. By the Division algorithm, there are integers q, r with $0 \leq r < d$ so that $a = qd + r = q(ax + by) + r$. Therefore, $r = a(1 - qx) + b(-qy)$ is another linear combination of a, b and it is less than d.

By the minimality of d, we must have $r = 0$, and thus d divides a. A symmetric argument guarantees d divides b.

So, d is a common divisor of a, b. Moreover, any common divisor c of a, b divides any linear combination of a, b; in particular, c divides d, and so $c \leq d$. Thus $d = \gcd(a, b)$. ∎

Problem 3. The *Euclidean Algorithm* is the following sequence of operations. Let $a, b \in \mathbb{Z}$ with $b > 0$. Repeatedly apply the Division Algorithm to the divisor and remainder of the previous division until the remainder is zero. In other words:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned}$$

For this problem:

(a) Prove that the Euclidean Algorithm terminates.

(b) Prove that the last nonzero remainder is $\gcd(a, b)$.

(c) Explain how the Euclidean Algorithm allows for the computation of the integers x, y in Bezout's identity.

Proof.

(a) Notice that $r_{j+1} < r_j$ because r_{j+1} is the remainder of something divided by r_j. Similarly, $r_1 < b$. So what we have is a strictly decreasing chain of nonnegative integers $b > r_1 > r_2 > \cdots \geq 0$. Clearly, this chain must terminate at zero after at most b steps. Thus the Euclidean Algorithm terminates.

(b) Notice that if b divides a, then $r_1 = 0$ and $\gcd(a, b) = b$ (here we view b as r_0, i.e., the "remainder" preceding r_1). Now, suppose b does not divide a so that $r_1 \neq 0$. Notice that the first equation guarantees that r_1 is a linear combination of a, b, and the second equation guarantees that r_2 is a linear combination of b, r_1, and hence also a linear combination of a, b. We will prove by strong induction that r_n is a linear combination of a, b. To this end, let $n \geq 3$ and suppose for every $j < n$, r_j is a linear combination of a, b. By the equation $r_{n-2} = r_{n-1} q_n + r_n$, we can easily see that r_n is a linear combination of r_{n-1} and r_{n-2}, which, by strong induction, are themselves linear combinations of a, b. Therefore r_n is a linear combination of a, b.

Finally, consider the last nonzero remainder r_n. Notice that r_n divides r_{n-1}, and therefore r_n divides $r_{n-2} = r_{n-1}q_n + r_n$, and so on up the chain. By another induction argument we can conclude r_n divides b *and* a. So, r_n is a linear combination of a, b which is also a common divisor. By Bezout's identity, it must be the *greatest* common divisor, hence $r_n = \gcd(a, b)$.

(c) In the proof of the preceding item, we remarked that each remainder is a linear combination of the previous two. Starting with r_n and expanding these linear combinations until we reach a, b will let us calculate the integers x, y in Bezout's identity.

■

Problem 4. The purpose of this problem is to analyze the efficiency of the Euclidean Algorithm. This necessitates a quick study of the Fibonacci sequence. Let $F_0 = 0$, $F_1 = 1$, and for all $n > 1$, define $F_n = F_{n-1} + F_{n-2}$; this is the *Fibonacci sequence.* In particular, the Fibonacci sequence is a linear recursion with constant coefficients. Let $\varphi = \frac{1+\sqrt{5}}{2}$ denote the *golden ratio.*

(a) Prove that the Fibonacci sequence is generated by the formula

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}},$$

and hence $F_n = \lceil \varphi^n \rceil$.

(b) Prove that that number of divisions required in the Euclidean Algorithm is at most $\log_\varphi b + 1$.

(c) Show that the above bound is optimal. That is, for any positive integer n, find positive integers a, b with $n > \log_\varphi b$ for which the Euclidean Algorithm applied to a, b requires n divisions.

Proof.

(a) Linear homogeneous recurrence relations with constant coefficients always have closed form solutions which are linear equations of exponential functions where the bases are roots of the characteristic equation; why? linear algebra. This is almost identical in nature to the solution of linear homogeneous differential equations with constant coefficients.

In the case of the Fibonacci sequence, the characteristic equation is $r^2 = r+1$, and solving for r we find $r = \frac{1\pm\sqrt{5}}{2}$. That is, $r = \varphi, 1-\varphi$, but $1-\varphi = -\varphi^{-1}$ since φ is a solution to the characteristic equation. Therefore, we find that the general solution to the Fibonacci sequence is of the form:

$$F_n = c_1\varphi^n + c_2(-\varphi)^{-n}$$

for some constants c_1, c_2. To solve for these, we notice that

$$\begin{aligned} 0 &= F_0 = c_1 + c_2 \\ 1 &= F_1 = c_1\varphi + c_2(-\varphi^{-1}) = c_1\varphi + c_2(1-\varphi). \end{aligned}$$

Solving this system of equations we find $c_2 = -c_2$ and thus, $1 = c_1(2\varphi - 1) = c_1\sqrt{5}$. Therefore, we obtain Binet's formula

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}},$$

as desired.

(b) Consider the following question: what is the smallest possible value for b that takes n divisions (note: the value of a doesn't matter at all)? Clearly, the smallest possible value for b occurs when all the quotients (except the first and the last, since those don't matter) are 1. However, this leads to the remainders satisfying the Fibonacci recurrence relation. Therefore, b is a Fibonacci number. As long as we can show the required inequality holds for Fibonacci numbers, we will be finished. For this, see the next part of the problem.

(c) Let $n \in \mathbb{N}$. The number of divisions required to apply the Euclidean Algorithm to the pair F_{n+2}, F_{n+1} is n. Indeed, the divisions all have quotient one and remainder the previous Fibonacci number. That is,

$$\begin{aligned} F_{n+2} &= F_{n+1} + F_n \\ F_{n+1} &= F_n + F_{n-1} \\ &\vdots \\ F_2 &= F_1 + F_0. \end{aligned}$$

$$\log \varphi F_{n+1} = \log_\varphi \left(\varphi^{n+1} - (-\varphi^{-(n+1)})\right) - \log_\varphi \sqrt{5} \approx n - 0.67.$$

■

Problem 5. Suppose that p, q are primes, $n = pq$ and e is a positive integer for which $\gcd(e, \operatorname{lcm}(p-1, q-1)) = 1$.

(a) Explain how to find a d for which $de \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$.

(b) Prove that $m^{ed} \equiv m \pmod{n}$. (This is Exercise 1 in Chapter 1, *hint: Fermat's Little Theorem*)

Proof.

(a) Note that $\gcd(e, \operatorname{lcm}(p-1, q-1) = 1$, and therefore by Bezout's identity, there are integers d, k for which $de + k\operatorname{lcm}(p-1, q-1) = 1$. Thus, this d satisfies $de \equiv 1 \pmod{\operatorname{lcm}(p-1, q-1)}$. By a previous problem, we can find this using the Euclidean Algorithm.

(b) By the Chinese Remainder Theorem, $m^{ed} \equiv 1 \pmod{n}$ if and only if $m^{ed} \equiv 1 \pmod{p}$ and $m^{ed} \equiv 1 \pmod{q}$. By symmetry, it suffices to prove it for p alone. The case $m \equiv 0 \pmod{p}$ is trivial, so assume $m \not\equiv 0 \pmod{p}$. Then

$$m^{ed} = m \cdot (m^{p-1})^k \equiv m \pmod{p},$$

where the congruence is due to Fermat's Little Theorem.

■

Problem 6. Exercise 4(a)–(d) of Chapter 1: Kid Krypto.

Proof. As in the statement of the problem, let $a, b, a', b' \in \mathbb{Z}$ and define

$$\begin{aligned} M &= ab - 1 && (1)\\ e &= a'M + a && (2)\\ d &= b'M + b && (3)\\ n &= \frac{ed-1}{M} = a'b'M + ab' + a'b + 1 && (4)\\ (n, e) &= \text{public key} && (5)\\ d &= \text{private key}. && (6) \end{aligned}$$

Encryption of a message m into a ciphertext c is given by $c \equiv em \pmod{n}$. Decryption of the ciphertext is given by $m \equiv dc \pmod{n}$.

(a) We begin by verifying that decryption actually works. For this, notice that $dem = m + (de - 1)m = m + Mmn$. Therefore,

$$dc \equiv dem \pmod{n} \equiv m \pmod{n}.$$

(b) You make digital signatures in essentially the same way it is done with RSA. That is, take a message m (or just a hash of it) that you want to sign, and apply your private key to it (in this case, multiply by $d \pmod{n}$. The recipient then verifies the signature by applying your public key (in this case, multiplying by $e \pmod{n}$. This works because, just like in RSA, the encryption and decryption operations are commutative.

(c) To break the system, note that e is a unit in $\mathbb{Z}/n\mathbb{Z}$ (since it is relatively prime to n). So, it suffices to compute the inverse d in this multiplicative group. However, that just amounts to finding a d such that $de = 1 + nk$ for some $k \in \mathbb{Z}$, but $d, -k$ are then just the integers in Bezout's identity, which we already proved we can find quickly and easily using the Euclidean Algorithm. Thus the private key is easily obtained from the public key.

(d) Suppose that an adversary can crack this cryptosystem for any choice of a, b, a', b'. Now let r, s be integers with $\gcd(r, s) = 1$. Then by Bezout's identity there exist integers x, y for which $rx + sy = 1$. Applying the division algorithm we find integers a, a' and b, b' satisfying

$$\begin{aligned} r &= a'(-y) + a \\ x &= b'(-y) + b. \end{aligned}$$

Then, with these choices of a, b, a', b', we find $n = s, e = r$. Breaking the cryptosystem yields d, which is x, and this also allows us to find y. Therefore we can find the integers in Bezout's identity.

■