Algebraic Cryptography
Homework 5

Due Wednesday, 25 October 2017

We begin with a bit more number theory, because it came up in our algebra material.

Exercise 1. Prove that $\operatorname{lcm}(j,n)\gcd(j,n) = nj$. If you choose to use the Fundamental Theorem of Arithmetic, you should first prove that; but there is an easier way.

To prove the first exercise, we will establish a few basic lemmas.

Lemma 1. *For any nonzero integers a, b, the integers $\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}$ are relatively prime.*

Proof. Let c be any common divisor of $\frac{a}{\gcd(a,b)}$ and $\frac{b}{\gcd(a,b)}$. Thus $\frac{a}{\gcd(a,b)} = ck$ and $\frac{a}{\gcd(a,b)} = cl$, hence $a = (c\gcd(a,b))k$ and $n = (c\gcd(a,b))l$. Thus $c\gcd(a,b)$ is a common divisor of a, b, and therefore $c = 1$. ■

Lemma 2. *Suppose that a, b are relatively prime integers that each divide some integer m, then ab also divides m.*

Proof. We prove this using Bezout's identity. Indeed, since a, b are relatively prime, then $1 = \gcd(a,b) = ax + by$ for some integers x, y. Also, $m = ak$ and $m = bl$ for some integers k, l. Thus $m = max + mby = blax + akby = ab(lx + ky)$ and hence ab divides m. ■

Lemma 3. *If a, b, c are integers, then $\operatorname{lcm}(ca, cb) \geq c\operatorname{lcm}(a,b)$.*

Proof. Let k be any common multiple of ca, cb, so that $k = car = cbs$ for some integers r, s. Then $\frac{k}{c} = ar = bs$ is an integer and a common multiple of a, b. Thus $\frac{k}{c} \geq \operatorname{lcm}(a,b)$ and hence $k \geq c\operatorname{lcm}(a,b)$. Therefore $\operatorname{lcm}(ca, cb) \geq c\operatorname{lcm}(a,b)$. ■

Proof. Clearly, Since $\frac{n}{\gcd(n,j)}$ and $\frac{j}{\gcd(n,j)}$ are integers, it is clear that $\frac{nj}{\gcd(j,n)}$ is a common multiple of n, j, and therefore $\operatorname{lcm}(n,j) \leq \frac{nj}{\gcd(j,n)}$, so it suffices to prove the reverse inequality. Note that by Lemma 1, $\gcd\left(\frac{n}{\gcd(n,j)}, \frac{j}{\gcd(n,j)}\right) = 1$.

Then by Lemma 2, any multiple of both $\frac{n}{\gcd(n,j)}, \frac{j}{\gcd(n,j)}$ is also a multiple of their product. Thus

$$\operatorname{lcm}\left(\frac{n}{\gcd(n,j)}, \frac{j}{\gcd(n,j)}\right) \geq \frac{nj}{\gcd(n,j)^2}.$$

By Lemma 3, we find

$$\operatorname{lcm}(n,j) \geq \gcd(n,j) \operatorname{lcm}\left(\frac{n}{\gcd(n,j)}, \frac{j}{\gcd(n,j)}\right) \geq \frac{nj}{\gcd(n,j)}. \qquad \blacksquare$$

Problem 2. Let $\varphi : \mathbb{N} \to \mathbb{N}$ denote Euler's totient function. That is, $\varphi(n)$ denotes the number of positive integers less than or equal to n which are relatively prime to n. We encountered this function before when reducing the RSA problem to the Integer Factorization Search problem in polynomial time. Since you were unfamiliar with it, I thought it would be good for you to review the basic properties.

(a) Prove that $\varphi(p^k) = p^k - p^{k-1}$ for any prime p.

(b) Prove that
$$\sum_{d|N} \varphi(d) = N.$$

(c) Prove that φ is *multiplicative.* That is, prove that if $\gcd(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Because we will use it below, we provide a quick proof of the Chinese Remainder Theorem. We only prove the case of two relatively prime positive integers, but this can easily be bootstrapped by induction to a finite collection of relatively prime positive integers.

Theorem 4 (Chinese Remainder Theorem)**.** *Let m, n be relatively prime positive integers. The map $\psi : k \mapsto \big(k \pmod m, k \pmod n\big)$ is a ring isomorphism between $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$.*

Proof. That ψ is a ring homomorphism follows easily from the fact that m, n divide mn. We leave checking that to the reader. Note: in general the standard map $\mathbb{Z}_r \to \mathbb{Z}_s$ is *not* a homomorphism.

To see that ψ is an isomorphism, we note that $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ both have mn elements. Then since these are finite sets with the same elements, it suffices to prove ψ is injective (for then it must also be surjective), and since it is a homomorphism, it suffices to prove the kernel is trivial. To this end, suppose $k \in \mathbb{Z}_{mn}$ and $\varphi(k) = (0,0)$. Then this means that n divides k and m divides k. By Lemma 2, we find that mn divides k, or in other words, $k = 0$. Thus $\ker \psi = \{0\}$ and so ψ is injective. $\blacksquare$

Proof. (a) Let p be a prime and k a positive integer. Then there are p^k integers in the interval $[1, p^k]$. Moreover, for an integer a, $\gcd(a, p^k) > 1$ if and only if p divides a. So, it suffices to count the number of multiples of p in this interval, of which there are clearly p^{k-1}. Finally, the number of integers in this interval which are relatively prime to p^k must be $\varphi(p^k) = p^k - p^{k-1}$.

(b) We will partition the interval $[1, N]$ in the following manner. For $d \mid N$, set $N_d := \{x \in [1, N] \mid \gcd(x, N) = d\}$. Clearly, $[1, N]$ is the disjoint union of N_d for $d \mid N$. We will prove that $|N_d| = \varphi\big(\frac{N}{d}\big)$. Indeed, notice that if $x \in N_d$, then $\frac{x}{d} \in \big[1, \frac{N}{d}\big]$ and by Lemma 1, $\gcd\big(\frac{x}{d}, \frac{N}{d}\big) = 1$. Therefore $|N_d| \leq \varphi\big(\frac{N}{d}\big)$. For the other direction, suppose that $y \in \big[1, \frac{N}{d}\big]$ and $\gcd\big(y, \frac{N}{d}\big) = 1$. Then $yd \in [1, N]$ and $\gcd(yd, N) = d$ (d is clearly a common divisor, and it can't be greater without $y, \frac{n}{d}$ having a common divisor). Thus $\varphi\big(\frac{N}{d}\big) \leq |N_d|$. Finally, notice that $d \mapsto \frac{N}{d}$ is a bijection of the divisors of N in $[1, N]$. Putting all this together we find

$$N = \sum_{d|N} |N_d| = \sum_{d|N} \varphi\left(\frac{N}{d}\right) = \sum_{d|N} \varphi(d).$$

(c) The map $\psi : k \mapsto \big(k \pmod{n}, k \pmod{m}\big)$ is a ring homomorphism from $\mathbb{Z}_{mn} \to \mathbb{Z}_n \times \mathbb{Z}_m$. In this problem, we always works with the least *positive* residues, so $\mathbb{Z}_n$ consists of the values $\{1, \ldots, n\}$. Let $k = k_n n + r_n$ and $k = k_m m + r_m$, where $r_n = k \pmod{n}$ and $r_m = k \pmod{m}$. Suppose k is relatively prime to mn. Then by Bezout's identity, there are integers x, y so that $kx + mny = 1$. Therefore,

$$1 = (k_n n + r_n)x + mny = r_n x + n(k_n + my).$$

Therefore, by Bezout's identity, $\gcd(r_n, n) = 1$. Similarly, $\gcd(r_m, m) = 1$.

The Chinese Remainder Theorem guarantees that the above map ψ is a bijection. Let N, M denote the sets of integers in $[1, n], [1, m]$ which are relatively prime to n, m, respectively. Note that N, M have $\varphi(n), \varphi(m)$ elements respectively. Then the previous paragraph guarantees that $\{k \in [1, mn] \mid \gcd(k, mn) = 1\} \subseteq \psi^{-1}(N \times M)$, and the right-hand set has $\varphi(n)\varphi(m)$ elements. Therefore, $\varphi(nm) \leq \varphi(n)\varphi(m)$.

Now suppose that $\gcd(k, mn) > 1$. Let p be a prime dividing $\gcd(k, mn)$. Then p divides mn so p divides either m or n. Without loss of generality, suppose p divides m. Since $r_m = k - k_m m$, p also divides r_m. Therefore, $\gcd(r_m, m) \geq p > 1$. This proves that $\psi^{-1}(N \times M) \subseteq \{k \in [1, mn] \mid \gcd(k, mn) = 1\}$, and therefore $\varphi(n)\varphi(m) \leq \varphi(nm)$.

Even though we have completed the proof, we remark that the last paragraph did not actually require that m, n be relatively prime, only that $\psi([1, mn])$ contains $N \times M$, which is certainly does. Therefore, in general $\varphi(nm) \geq \varphi(n)\varphi(m)$. ∎

Now for the algebra.

Exercise 3. Suppose $\mathbb{F}$ is a finite field with q elements, which we will henceforth denote $\mathbb{F}_q$ (we will prove uniqueness up to isomorphism later). Prove that $q = p^n$ for some $n \in \mathbb{N}$ and some prime p.

Proof. Since $\mathbb{F}_q$ is a finite field, it cannot have characteristic zero (otherwise it would contain $\mathbb{Q}$, which is infinite). Thus $\mathbb{F}_q$ has prime characteristic p, and therefore contains $\mathbb{F}_p$ as a subfield. Recall that whenever we have an inclusion of fields, we can view the larger one as a vector space over the smaller one. Thus $\mathbb{F}_q$ is an $\mathbb{F}_p$-vector space of some dimension n, which is necessarily finite since $\mathbb{F}_q$ is finite. Let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis for $\mathbb{F}_q$ over $\mathbb{F}_p$. Then the function $\mathbb{F}_p^n \to \mathbb{F}_q$ given by $(c_1, \dots, c_n) \mapsto \sum_{k=1}^n c_k v_k$ is a bijection since $\mathcal{B}$ is a basis. Therefore $q = p^n$. ∎

Problem 4. Prove that the number of k-th roots of unity in $\mathbb{F}_{p^f}$ is equal to $\gcd(k, p^f - 1)$.

Proof. Let $d = \gcd(k, p^f - 1)$. Since $\mathbb{F}_{p^f}^*$ is cyclic, generated by g, and has order $p^f - 1$ divisible by d, it has d d-th roots of unity. Indeed, they are precisely the elements $g^{\frac{j(p^f-1)}{d}}$ for $1 \leq j \leq d$. Clearly, any k-th root is also a d-th root, but the converse holds as well. Indeed, since $d = kx + (p^f - 1)y$, if $a \in \mathbb{F}_{p^f}^*$ is a k-th root of unity, then

$$a^d = a^{kx+(p^f-1)y} = (a^k)^x + (a^{p^f-1})^y = 1.$$ ∎

Proof. A k-th root of unity in $\mathbb{F}_{p^f}$ is a nonzero element x such that $x^k = 1$. Recall that $\mathbb{F}_{p^f}^*$ is cyclic and therefore generated by some element g of order necessarily equal to $p^f - 1$. So $\mathbb{F}_{p^f}^* = \{g^j \mid 1 \leq j \leq p^f - 1\}$. Then the question is, for which $1 \leq j \leq p^f - 1$ is $(g^j)^k = 1$? But $(g^j)^k = 1$ if and only if the order of g^j, which is $\frac{p^f-1}{\gcd(j,p^f-1)}$, divides k. That is, if $m(p^f - 1) = k\gcd(j, p^f - 1)$ for some m. In other words, if $p^f - 1$ divides $k\gcd(j, p^f - 1)$. This happens if and only if $\frac{p^f-1}{\gcd(k,p^f-1)}$ divides $\gcd(j, p^f - 1)$. Finally, we conclude that ∎

Problem 5. Suppose that $\alpha \in \mathbb{F}_{p^2}$ is a root of the polynomial $x^2 + ax + b \in \mathbb{F}_p[x]$.

(a) Prove that α^p is also a root of this polynomial.

(b) Prove that if $\alpha \notin \mathbb{F}_p$, then $a = -\alpha - \alpha^p$ and $b = \alpha^{p+1}$.

(c) Prove that if $\alpha \notin \mathbb{F}_p$ and $c, d \in \mathbb{F}_p$, then $(c\alpha + d)^{p+1} = d^2 - acd + bc^2$ (which is an element of $\mathbb{F}_p$).

(d) Let i be a square root of -1 in $\mathbb{F}_{19^2}$. Use part (c) to find $(2 + 3i)^{101}$ (that is, write it in the form $a + bi$ for $a, b \in \mathbb{F}_{19}$.

Proof. Suppose that $\alpha \in \mathbb{F}_p^2$ is a root of the polynomial $x^2 + ax + b \in \mathbb{F}_p[x]$.

(a) Since $a, b \in \mathbb{F}_p$, we know that $a^p = a$ and $b^p = b$ by Fermat's Little Theorem. Moreover, since the Frobenius map is a homomorphism, we find that

$$(\alpha^2 + a\alpha + b)^p = (\alpha^2)^p + a^p\alpha^p + b^p = (\alpha^p)^2 + a\alpha^p +_b .$$

Thus, if α is a root of this quadratic, then the left-hand side is zero, and therefore α^p is also a root.

(b) If $\alpha \notin \mathbb{F}_p$, then $\alpha^p \neq \alpha$ since $\mathbb{F}_p$ is precisely the roots of $x^p - x$. Thus we can factor the quadratic as

$$x^2 + ax + b = (x - \alpha)(x - \alpha^p) = x^2 + (-\alpha - \alpha^p)x + \alpha^{p+1}.$$

(c) Suppose $\alpha \notin \mathbb{F}_p$ and $c, d \in \mathbb{F}_p$. Then $c^p = c$ and $d^p = d$ by Fermat's Little Theorem, and

$$\begin{aligned}
(c\alpha + d)^{p+1} &= (c\alpha + d)^p(c\alpha + d) \\
&= (c\alpha^p + d)(c\alpha + d) \\
&= c^2\alpha^{p+1} + cd(\alpha + \alpha^p) + d^2 \\
&= bc^2 - acd + d^2.
\end{aligned}$$

(d) Since $i = \sqrt{-1} \in \mathbb{F}_{19^2} \setminus \mathbb{F}_{19}$, in the notation of part (b) and (c), we have $a = 0$, $b = 1$ and $c = 2$, $d = 3$.

$$\begin{aligned}
(2 + 3i)^{101} &= (2 + 3i)^{20\cdot 5+1} \\
&= \left((2 + 3i)^{19+1}\right)^5(2 + 3i) \\
&= (2^2 + 3^2)^5(2 + 3i) \\
&= 14(2 + 3i) \\
&= 9 + 4i.
\end{aligned}$$

■

Problem 6. Consider $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ (i.e., the group of units of this ring; the set of integers relatively prime to p^α with multiplication mod p^α) where p is prime.

(a) Suppose $p > 2$, and let g be an integer that generates $\mathbb{F}_p^*$. Let α be any integer greater than 1. Prove that either g or $(p+1)g$ generates $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. Thus the latter is also a *cyclic group*.

(b) Prove that if $\alpha > 2$, then $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ is *not* cyclic, but that the number 5 generates a *subgroup* consisting of half of its elements, namely those which are $\equiv 1 \pmod 4$.

Proof. (a) Suppose $p > 2$ and g is an integer that generates $\mathbb{F}_p^*$, and let $\alpha > 1$. We claim that the orders of $g, g(p+1)$ in $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ are each divisible by $(p-1)$. Indeed, suppose that $g^j \equiv 1 \pmod{p^\alpha}$. Then $g^j \equiv 1 \mod p$ since $p \mid p^\alpha$, and therefore $(p-1) \mid j$ since g has order $(p-1)$ in $\mathbb{F}_p^*$. A similar argument holds for the order of $g(p+1)$ as long as you recognize that $(p+1) \equiv 1 \pmod{p}$.

Our next claim is that either g^{p-1} or $(g(p+1))^{p-1}$ is not congruent to $1 \pmod{p^2}$. Indeed, note that by the binomial expansion of $(p+1)^{p-1}$, we see that it is congruent to $p+1 \pmod{p^2}$. Therefore, either $g^{p-1} \not\equiv 1 \pmod{p^2}$, or $(g(p+1))^{p-1} \equiv p+1 \pmod{p^2} \not\equiv 1 \pmod{p^2}$. So, pick whichever one is *not* congruent to $1 \pmod{p^2}$. For clarity, we will just call this element h. Then from the proof in the previous paragraph we can conclude $h^{p-1} \equiv 1 \pmod{p}$, and so $h^{p-1} = 1 + g_1 p$, for some integer g_1, but from this paragraph, $h^{p-1} \not\equiv 1 \pmod{p^2}$, and therefore p does not divide g_1, so $\gcd(g_1, p) = 1$.

Suppose that $h^j \equiv 1 \pmod{p^\alpha}$. By the first paragraph, $(p-1) \mid j$, and so $j = (p-1)k$ for some integer k. Thus $(1 + g_1 p)^k = h^{(p-1)k} = h^j \equiv 1 \pmod{p^\alpha}$. Expanding the left-hand side with the binomial theorem we obtain

$$1 + kg_1 p + \sum_{n=2}^{k} \binom{k}{n} g_1^n p^n \equiv 1 \pmod{p^\alpha}.$$

Thus p^α divides

$$x = kg_1 p + \sum_{n=2}^{k} \binom{k}{n} g_1^n p^n.$$

We will prove by induction on m that p^m divides k up to $m = \alpha - 1$.

For the base case, notice that since $\alpha > 1$ and p^α divides x, so also does p^2. Moreover, p^2 obviously divides all the terms after the first one in x, so p^2 must also divide $kg_1 p$. Therefore p divides kg_1, and since p is prime it divides k since it does not divide g_1.

For the inductive step, suppose that $1 \le m < \alpha - 1$ and p^m divides k. Since $m + 2 \le \alpha$ and p^α divides x, so also does p^{m+2} divides x. We claim that p^{m+2} divides all terms after the first one. Indeed, for $2 \le n \le k-1$, p^m divides k which in turn divides $\binom{k}{n}$, and p^2 divides p^n, and therefore p^{m+2} divides $\binom{k}{n} g_1^n p^n$. For the last term, notice that $p^k = p^{p^m l}$ for some integer l, and then notice that $p^m \ge m + 2$ for any prime $p > 2$ (this is where the proof breaks for $p = 2$! Kind of subtle huh?). Thus p^{m+2} divides the last term $g_1^k p^k$. Finally, since p^{m+2} divides x and every term of x besides the first, it must also divide $kg_1 p$. Since $\gcd(g_1, p) = 1$, this implies that p^{m+1} divides k. By induction we have established that $p^{\alpha-1}$ divides k.

In conclusion, if $h^j \equiv 1 \pmod{p^\alpha}$, then $j = (p-1)k$ and $p^{\alpha-1}$ divides k, and therefore $p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$ divides j. Thus the order of h is at least $(p-1)p^{\alpha-1}$, but this is the order of the group $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$, so h generates the group.

(b) Note that the order of $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ is $2^{\alpha-1}$ (since it just consists of the odd integers less than 2^α). Any cyclic group has at most one element of order

2. Indeed, consider $\langle g \rangle$ with g of order n. Then g^j has order $\frac{n}{\gcd(n,j)} = 2$ if and only if $n = 2\gcd(n,j)$. Thus n is even and $\gcd(n,j) = \frac{n}{2}$, but the only $1 \leq j \leq n$ for which this occurs is $j = \frac{n}{2}$.

So, if $\alpha > 2$, then $2^{\alpha-1} \pm 1$ are distinct elements of $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$. Moreover, $(2^{\alpha-1} \pm 1)^2 = 2^\alpha \pm 2 \cdot 2^{\alpha-1} + 1 \equiv 1 \pmod{2^\alpha}$. Therefore $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ has two elements of order 2, and hence cannot be cyclic.

However, we will prove that 5 has order $2^{\alpha-2}$ in $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$. Notice that $5 = 1 + 2^2$, and suppose $5^k \equiv 1 \pmod{2^\alpha}$. Then 2^α divides

$$x = k2^2 + \sum_{n=2}^{k} \binom{k}{n} 2^{2n}.$$

An induction argument nearly identical to the previous one guarantees that k divides $2^{\alpha-2}$. Therefore the order of 5 is $2^{\alpha-2}$ (since it can't have order $2^{\alpha-1}$ since it can't be a generator since the group isn't cyclic).

■