Math 4613 - Cryptography - Practice Midterm
SOLUTIONS
Paul L. Bailey
October 30, 2007

Part I: Mathematics

Problem 1. Complete the following definitions.

(a) Let $f : A \to B$. We say that f is *surjective* if ...

for every $b \in B$ there exists $a \in A$ such that $a \in A$.

(b) Let $a, n \in \mathbb{Z}$ with $n \geq 2$. The *congruence class of a modulo n* is ...

the set $[a]_n = \{b \in \mathbb{Z} \mid n \text{ divides } a - b\}$.

(c) Let $(A, *)$ be a magma, and let $B, C \subset A$. Then $B * C$ means ...

$\{x \in A \mid x = bc \text{ for some } b \in B, c \in C\}$.

(d) Let G be a finite group and let $g \in G$. The *order* of g is ...

the smallest positive integer n such that $g^n = 1$.

(e) Let R be a ring and let $a \in R$. We say that a is *invertible* if ...

there exists $b \in R$ such that $ab = ba = 1$.

Problem 2. Let $a, b, c, d, n \in \mathbb{Z}$ with $n \geq 2$. Suppose $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Show that $ab \equiv cd \pmod{n}$.

Solution. Since $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, n divides $a - c$ and n divides $b - d$. Thus there exist $x, y \in \mathbb{Z}$ such that $a - c = xn$ and $b - d = yn$. Thus $a = xn + c$ and $b = yn + d$; multiplying these gives

$$ab = xyn^2 + xnd + cyn + cd = n(xyn + xd + cy) + cd.$$

Thus $ab - cd = n(xyn + xd + cy)$, so n divides $ab - cd$. Therefore, $ab \equiv cd \pmod{n}$. □

Problem 3. Find the inverse of $\overline{123}$ in $\mathbb{Z}_{127}$.

Solution. We use the Euclidean algorithm to compute that

$$\begin{aligned} 127 &= 123(1) + 4 \\ 123 &= 4(30) + 3 \\ 4 &= 3(1) + 1 \end{aligned}$$

Thus

$$\begin{aligned} 1 &= 3(-1) + 4(1) \\ &= 4(31) + 123(-1) \\ &= 123(-32) + 127(31) \end{aligned}$$

Reducing this equation modulo 127and computing in $\mathbb{Z}_{127}$, we have, since $\overline{127} = \overline{0}$,

$$\overline{1} = \overline{123}(\overline{-32}) + \overline{127}(\overline{31}) = \overline{123}(\overline{95}).$$

Thus the multiplicative inverse of $\overline{127}$ is $\overline{95}$. □

Problem 4. Find the inverse of $A = \begin{bmatrix} \overline{5} & \overline{2} \\ \overline{11} & \overline{9} \end{bmatrix}$ in $\mathcal{M}_{2\times 2}(\mathbb{Z}_{17})$.

Solution. We use the fact that, if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a, b, c, d \in R$ for any ring R, is invertible if and only if $\det(A) = ad - bc$ is invertible in R, in which case

$$A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

We compute in $\mathbb{Z}_{17}$, without bars (for readability). In our case,

$$\det(A) = 5(9) - 2(11) = 45 - 22 = 23 = 6,$$

which is invertible modulo 17; the inverse of 6 in $\mathbb{Z}_{17}$ is 3. Thus

$$A^{-1} = 3 \begin{bmatrix} 9 & -11 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & 1 \\ 11 & 15 \end{bmatrix}.$$

□

Problem 5. Find all $x \in \mathbb{Z}_{23}$ such that $x^2 + \overline{16}x - \overline{11} = \overline{0}$.

Proof. The idea is to rewrite the equation, switching signs modulo 23 as necessary in order to simplify the equation. Computing modulo 23, we have

$$x^2 + 16x - 11 = x^2 - 7x + 12 = (x-3)(x-4) = 0.$$

Since $\mathbb{Z}_{23}$ is a field, the product of two elements is zero if and only if one of them is zero. Thus $x = 3$ or $x = 4$ are the only solutions. □

Problem 6. Let R be a ring and let $S, T \leq R$. Show that $S \cap T \leq R$.

Proof. To show that $S \cap T$ is a subring, we verify properties **(S0)** through **(S1)**.

(S0) Since S and T are subrings, $1 \in S$ and $1 \in T$. Thus $1 \in S \cap T$.

(S1) Let $a, b \in S \cap T$. Then $a, b \in S$ and $a, b \in T$. Since S and T are subrings, $a + b \in S$ and $a + b \in T$. Thus $a + b \in S \cap T$.

(S2) Let $a \in S \cap T$. Then $a \in S$ and $a \in T$. Since S and T are subrings, $-a \in S$ and $-a \in T$. Thus $-a \in S \cap T$.

(S3) Let $a, b \in S \cap T$. Then $a, b \in S$ and $a, b \in T$. Since S and T are subrings, $ab \in S$ and $ab \in T$. Thus $ab \in S \cap T$. □

Problem 7. Let G be a group and let $H, K \leq G$, with $K \leq H$. Show that

$$[G : K] = [G : H][H : K].$$

Proof. Since $H, K \leq G$ and $K \leq H$, Lagrange's Theorem tells us that

$$|G| = |H|[G : H], \quad |G| = |K|[G : K], \quad \text{and} \quad |H| = |K|[H : K].$$

Thus

$$|K|[G : K] = |H|[G : H] = |K|[H : K][G : H].$$

Cancelling $|K|$ and commuting gives $[G : K] = [G : H][H : K]$. □

Problem 8. Let G be a group and let $H, K \leq G$. Show that

$$[G : H \cap K] = [G : H][H : H \cap K].$$

Proof. Apply the previous problem with $H \cap K$ replaces K. □

Problem 9. Let the RSA modulus be $n = 713$ and the RSA encryption exponent is $e = 29$, find the RSA decryption exponent d.

Solution. We require that $ed \equiv 1 \pmod{\phi(n)}$.

To find $\phi(n)$, we factor 713. Let $p = 31$ and $q = 23$; then $n = pq$. Thus $\phi(n) = (p-1)(q-1) = 660$.

Now use the euclidean algorithm to find the inverse d of $e = 29$ in $\mathbb{Z}_{660}$.

$$\begin{aligned} 660 &= 29(22) + 22 \\ 29 &= 22(1) + 7 \\ 22 &= 7(3) + 1 \\ 1 &= 7(-3) + 22(1) \\ &= 22(4) + 29(-3) \\ &= 29(-91) + 660(4) \end{aligned}$$

Thus the inverse of 29 in $\mathbb{Z}_{660}$ is $d = -91 = 569$. □

For the next problem, we first produce a lemma.

Lemma 1. *Let G be a group with $H, K \leq G$. If $H \cap K = \{1\}$ and $h \in H$, then the elements of $\langle h \rangle$ are in different cosets of K in G.*

Proof. Suppose that $h^i K = h^j K$. Then $h^i k_1 = h^j k_2$ for some $k_1, k_2 \in K$. Thus $h^{i-j} = k_2 k_1^{-1}$, so $h^{i-j} \in K$, so $h^{i-j} = 1$. Thus $h^i = h^j$. □

Lemma 2. *Let G be a group and $H \triangleleft G$. Let $g \in G$ have finite order. Then* $\operatorname{ord}(gH)$ *divides* $\operatorname{ord}(g)$.

Proof. In the group G/H, the identity is H. Let $n = \operatorname{ord}(g)$; then $(gH)^n = g^n H = 1H = H$, so $\operatorname{ord}(gH)$ divides n. □

Problem 10. Let G be a group and let $H \triangleleft G$. Suppose that $|G| = 588$ and $|H| = 21$.

(a) Show that H has an element of order 3.

(b) Show that all elements of order 3 in G are actually in H.

Proof. First, we use that the order of an element divides the order of the group.

(a) Suppose that H has no element of order 3. The only possible orders of elements in H are then 1 and 7. But H can only have one element of order 1, so it has 20 elements of order 7. The cyclic subgroups generated by these elements are either equal or intersect at the identity (since the intersection of subgroups is a subgroup, and 7 is prime), so the total number of elements of order 7 is divisible by 6 (which is the number of elements of order 7 in a cyclic subgroup of order 7). But 20 is not divisible by six.

(b) We factor $588 = 2^2 \cdot 3 \cdot 7^2$. So, $|G/H| = [G : H] = 588/21 = 2^2 \cdot 7 = 28$. If $g \in G$ is an element of order 3, then $(gH)^3 = g^3 H = H$, so $\operatorname{ord}(gH)$ divides 3. Also, $\operatorname{ord}(gH)$ divides 28, so $\operatorname{ord}(gH)$ divides $\gcd(3, 28) = 1$; thus $\operatorname{ord}(gH) = 1$, which implies that $g \in H$. □

Problem 11. Let B denote the set of bytes. Find the largest subset $K \subset B$ of keys on which the following functions $B \to B$ are bijective.

```
BYT ron(BYT byt,BYT key)
{ return byt + key; }

BYT bob(BYT byt,BYT key)
{ return byt * key; }

BYT ned(BYT byt,BYT key)
{ return byt / key; }

BYT tom(BYT byt,BYT key)
{ return byt & key; }

BYT sue(BYT byt,BYT key)
{ return byt | key; }

BYT tim(BYT byt,BYT key)
{ return byt ^ key; }

BYT rob(BYT byt,BYT key)
{ return byt << key; }

BYT ted(BYT byt,BYT key)
{ return bytrot(byt,key); }
```

Solution. `ron` is bijective on B
`bob` is bijective on B^*
`ned` is bijective on $\{1\}$
`tom` is bijective on $\{256\}$
`sue` is bijective on $\{0\}$
`tim` is bijective on B
`rob` is bijective on $\{0\}$
`ted` is bijective on B □