Exam 2009-11-30

(with solutions)

2010-11-26

Problem 1

For which values of the integer a does the following system have a solution.

$$x \equiv 2 \pmod{15}$$
$$x \equiv a \pmod{21}.$$

For the values of a with $1 \leq a \leq 5$: find all solutions of the above system.

Solution to Problem 1 (part 1/2)

Note that $\gcd(15,21) = 3$. The given equations imply $x \equiv 2 \pmod 3$ and $x \equiv a \pmod 3$, hence there is no solution unless $a \equiv 2 \pmod 3$.

On the other hand, when $a \equiv 2 \pmod 3$ the given system is equivalent to

$$x \equiv 2 \pmod{15}$$
$$x \equiv a \pmod 7,$$

and by the Chinese Remainder Theorem, this system has a unique solution modulo $7 \cdot 15 = 105$.

Thus the system has a solution precisely when $a \equiv 2 \pmod 3$.

For $a = 2$, the solution is obviously $x \equiv 2 \pmod{105}$.

Solution to Problem 1 (part 2/2)

In general, the revised system can be written

$$7x \equiv 14 \pmod{105}$$
$$15x \equiv 15a \pmod{105}.$$

Since $15 - 2 \cdot 7 = 1$, the second equation minus twice the first yields

$$x \equiv 15a - 28 \pmod{105}.$$

For $a = 5$ the result is

$$x \equiv 47 \pmod{105}.$$

Problem 2

Let $(n,e) = (187,7)$ be an RSA-public key pair. Find the private key d, and decrypt the ciphertext $c = 6$.

Solution: First, note that $187 = 11 \cdot 17$. So $\varphi(187) = \varphi(11)\varphi(17) = 10 \cdot 16 = 160$. The private key d is the inverse of e modulo 160.

We find it by the extended Euclidean algorithm. (In modified form. The Euclidean algorithm on the left, taken modulo 160 on the right.)

$$160 = 7 \cdot 22 + 6 \qquad 6 \equiv -22e \pmod{160}$$

$$7 = 6 + 1 \qquad 1 = 7 - 6 \equiv e + 22e = 23e \pmod{160}$$

so d=23. (Check: $7 \cdot 23 = 161 \equiv 1 \pmod{160}$)

The decryption of $c = 6$ is $m = c^{23} \bmod 161 = 6^{23} \bmod 187$. With the aid of a simple calculator you can find $6^{11} = 362797056 = 187 \cdot 1940091 + 39$, and so $6^{23} \equiv 39^2 \cdot 6 = 9126 = 187 \cdot 48 + 150 \equiv 150 \pmod{187}$, thus $m = 150$.

Problem 3

Use the Baby-Step Giant-Step method to solve the discrete logarithm problem

$$2^x \equiv 5 \pmod{101}.$$

Solution: Writing $x = 10i + j$ with $i, j \in \{0, 1, \ldots, 9\}$ we rewrite as

$$2^j \equiv 5 \cdot 2^{-10i} \pmod{101}.$$

Tabulate $2^j \bmod 101$:

j	1	2	3	4	5	6	7	8	9	10
2^j	2	4	8	16	32	64	27	54	7	14

Next, compute $2^{-10} \equiv 14^{-1} \equiv 65 \pmod{101}$ (check: $65 \cdot 14 = 910 \equiv 1 \pmod{101}$) and tabulate $5 \cdot 2^{-10i} \bmod 101$:

i	0	1	2
$5 \cdot 2^{-10i}$	5	22	16

and therefore $i = 2$, $j = 4$, $x = 24$.

Check: $2^{24} \equiv 14^2 \cdot 16 = 3136 = 31 \cdot 101 + 5 \equiv 5 \pmod{101}$.

Problem 4(a)

Let (p, α, β) be a public key to be used for ElGamal signatures. Let a be the corresponding private key, such that $\beta \equiv \alpha^a \pmod{p}$. Then ElGamal signatures are defined such that $(r, s) = (\alpha^k \bmod p, k^{-1}(m - ar) \bmod p - 1)$ is a signature on m, where k is some random number with $\gcd(k, p-1) = 1$.

(a) A signature is verified by checking if $\beta^r r^s \equiv \alpha^m \pmod{p}$. Show that a signature (r, s) on m, as described above, satisfies this equation.

Solution From $s = k^{-1}(m - ar) \bmod p - 1$ we get $m \equiv sk + ar \pmod{p-1}$, and therefore (using Fermat's little theorem in the first step)

$$\alpha^m \equiv \alpha^{sk+ar} = (\alpha^k)^s (\alpha^a)^r \equiv r^s \beta^r \pmod{p}.$$

Problem 4(b)

Let (p, α, β) be a public key to be used for ElGamal signatures. Let a be the corresponding private key, such that $\beta \equiv \alpha^a \pmod{p}$. Then ElGamal signatures are defined such that $(r, s) = (\alpha^k \bmod p, k^{-1}(m - ar) \bmod p - 1)$ is a signature on m, where k is some random number with $\gcd(k, p-1) = 1$.

(b) With public key $(p, \alpha, \beta) = (83, 2, 28)$ and private key $a = 10$, compute a signature on the message $m = 8$, using the value $k = 7$.

Solution to (b) First, $r = 2^7 \bmod 83 = 128 \bmod 83 = 45$.

Second, $k^{-1} \bmod 82 = 7^{-1} \bmod 82 = 47$. (Check: $7 \cdot 47 = 329 = 4 \cdot 82 + 1 \equiv 1 \pmod{82}$.)
So $s = k^{-1}(m - ar) \bmod p - 1 = 47 \cdot (8 - 10 \cdot 45) \bmod 82 = 54$.

The signature is $(r, s) = (45, 54)$.

Problem 5(a)

(a) Explain why and how one can find a factorization of $n = pq$, where p and q are different primes, using that two numbers x, y are known, such that

$$x^2 \equiv y^2 \pmod{n}$$

and

$$x \not\equiv \pm y \pmod{n}$$

Solution to (a) $x^2 \equiv y^2 \pmod{n}$ means $x^2 - y^2 = (x-y)(x+y)$ is a multiple of n. Thus $p \mid (x-y)(x+y)$, and therefore either $p \mid (x-y)$ or $p \mid (x+y)$ since p is a prime.

Say $p \mid (x-y)$. Then $q \nmid (x-y)$, for otherwise we would have $n \mid (x-y)$,
which contradicts $x \not\equiv y \pmod{n}$.
So we have $p \mid \gcd(x-y, n)$ and $q \nmid \gcd(x-y, n)$, and therefore $\gcd(x-y, n) = p$
(since the only divisors of n are 1, p, q, $pq = n$).

The argument in the case $p \mid (x+y)$ is the same, with y replaced by $-y$.

Problem 5(b)

(b) Explain (briefly) how and why coin flipping via the telephone works, using the idea of part (a).

Solution to (b)

Alice finds two large primes p and q and reveals their product n to Bob.
Bob picks a number x and sends $X = x^2 \bmod n$ to Alice.
Alice can compute square roots of X modulo p and modulo q (there are two possibilities in each case, for a total of four possibilities) and combine them using the Chinese remainder theorem (CRT) to get square roots of X modulo n.
She picks one of them, call it y, and sends it to Bob.
There is a 50% chance that $y \equiv \pm x \pmod{n}$, in which case Bob loses.
Otherwise, Bob uses x and y to factorize n and wins.

Problem 5(c)

(c) Find all solutions of $x^2 \equiv 1 \pmod{133}$

Solution to (c) Since $133 = 7 \cdot 19$ there will be four solutions. Two of them will be $\pm 1 \bmod 133$.

The other two will be $\pm x$, where $x \equiv -1 \pmod 7$, $x \equiv 1 \pmod{19}$, which we write in the equivalent form

$$\left.\begin{aligned} 19x &\equiv -19 \\ 7x &\equiv 7 \end{aligned}\right\} \pmod{133}$$

It is now useful to know $19^{-1} \bmod 7 = 5^{-1} \bmod 7 = 3$.
(By inspection – since $3 \cdot 5 = 15 \equiv 1 \pmod 7$.)
Dividing $3 \cdot 19 - 1$ by 7, we learn $3 \cdot 19 - 8 \cdot 7 = 1$, so we multiply the first congruence above by 3 and the second by 8 and subtract, getting

$$x \equiv -3 \cdot 19 - 8 \cdot 7 = -113 \equiv 20 \pmod{133}.$$

The four square roots of 1 modulo 133 are 1, 20, 113 and 132.

Problem 6(a)

(a) Consider the function $f(x) = \alpha^x \pmod{83}$ on $\{1, 2, \ldots, 82\}$. Show that the function is a permutation for $\alpha = 2$, but not a permutation for $\alpha = 3$.

Solution to (a) 83 is a prime, so $a^x \bmod 83$ depends only on $x \bmod 82$, by Fermat's little theorem.

The map is a permutation if and only if it is 1–1, that is if $\alpha^x \equiv \alpha^y \pmod{83}$ implies $x \equiv y \pmod{82}$. And this happens if and only if $\alpha^x \equiv 1 \pmod{83}$ implies $x \equiv y \pmod{82}$, which is equivalent to α being a primitive root modulo 83.

Since $82 = 2 \cdot 41$ and 41 is a prime (i.e., 83 is a safe prime and 41 is the corresponding Sophie Germain prime), $\alpha \in \mathbb{Z}_{83}^*$ is a primitive root modulo 83 if and only if $\alpha^2 \not\equiv 1 \pmod{83}$ and $\alpha^{41} \not\equiv 1 \pmod{83}$.

$\alpha = 2$ and $\alpha = 3$ clearly both satisfy the first requirement.

We find $2^{10} = 1024 \equiv 28 \pmod{83}$, hence $2^{41} \equiv 28^4 \cdot 2 \equiv 82 \pmod{83}$, and therefore 2 is a primitive root modulo 83.

On the other hand, we find $3^{10} = 59049 \equiv 36 \pmod{83}$, hence $3^{41} \equiv 36^4 \cdot 3 \equiv 1 \pmod{83}$, and therefore 3 is not a primitive root modulo 83.

Problem 6(b)

(b) Let p be a prime, and consider the function

$$g(x) = x^3 + 1 \pmod{p} \text{ on } \{0, 1, 2, \ldots, p-1\}.$$

Show that the function g is a permutation for $p = 401$ and for $p = 419$, but not a permutation for $p = 409$.

Solution to (b) This time, the question is about whether $x^3 + 1 \equiv y^3 + 1 \pmod{p}$ implies $x \equiv y \pmod{p}$. Clearly, $x^3 + 1 \equiv y^3 + 1 \pmod{p}$ implies $x^3 \equiv y^3 \pmod{p}$.

Since p is a prime, $x^3 \equiv 0 \pmod{p}$ if and only if $x \equiv 0 \pmod{p}$, so we only need to consider $x, y \not\equiv 0 \pmod{p}$. In this case, $x^3 \equiv y^3 \pmod{p}$ implies $(x/y)^3 \equiv 1 \pmod{p}$, so the given map is a permutation if and only if $z^3 \equiv 1 \pmod{p}$ implies $z \equiv 1 \pmod{p}$.

Every $z \in \mathbb{Z}_p^*$ has a period $r \geq 1$, and $r \mid (p-1)$. $z^3 \equiv 1 \pmod{p}$ is equivalent to $r \mid 3$, so $r = 1$ (in which case $z \equiv 1$) or $r = 3$, so the latter can happen only if $3 \mid (p-1)$.

For $p = 401$ and $p = 419$, $3 \nmid (p-1)$, so the map is a permutation in those cases.

For $p = 409$, however, $p - 1 = 3 \cdot 136$. The polynomial $u^{136} - 1$ can have at most 136 zeros modulo p, so there is some $u \in \mathbb{Z}_{409}^*$ with $u^{136} \not\equiv 1 \pmod{409}$. But then $z = u^{136}$ satisfies $z^3 = u^{148} \equiv 1 \pmod{409}$ by Fermat's little theorem, and the map is not a permutation.