MATH 430 Final Exam

Qilin Ye

November 20, 2020

Solution: Problem 1

One thing to notice is that $17^2 = 289 = 2 \cdot 144 + 1$. Therefore,

$$x^{173} \equiv 17 \pmod{144} \implies (x^{173})^2 = x^{346} \equiv 17^2 \equiv 1 \pmod{144}.$$

This first shows that $\gcd(x, 144) = 1$ since otherwise x^{346} cannot be of form $144k+1$, a number not divisible by any divisor of 144 other than 1. Therefore $x \in (\mathbb{Z}/144\mathbb{Z})^*$. Furthermore, by the congruence relation above we have $o(x) \mid 364$. On the other hand, the fact that $x \in (\mathbb{Z}/144\mathbb{Z})^*$ implies $o(x) \mid \varphi(144) = 48$. Therefore $o(x) \mid \gcd(364, 144) = 2$. Clearly $o(x) \neq 1$ since $1 = e \in (\mathbb{Z}/144\mathbb{Z})^*$ will never become 17 when raised to some power. Therefore $o(x) = 2$ and so $x^2 \equiv 1 \pmod{144}$. Thus,

$$x^{173} = (x^2)^{86} \cdot x \equiv 1 \cdot x \equiv 17 \pmod{144} \implies x \equiv 17 \pmod{144}$$

which gives our solution.

Solution: Problem 2

First we prime factorize $1104 = 2^4 \cdot 69$. Now, for convenience, we start by checking whether 2 is a witness:

$2^{69} \equiv 967 \not\equiv 1 \pmod{1105}$	condition 1 met, proceed
$2^{69} \equiv 967 \not\equiv -1 \pmod{1105}$	not failing condition 2, proceed
$2^{2\cdot 69} \equiv 259 \not\equiv -1 \pmod{1105}$	not failing condition 2, proceed
$2^{4\cdot 69} \equiv 781 \not\equiv -1 \pmod{1105}$	not failing condition 2, proceed
$2^{8\cdot 69} \equiv 1 \not\equiv -1 \pmod{1105}$	condition 2 met, `return true`

Indeed 2 is a strong witness, and we conclude that 1105 is composite.

Solution: Problem 3

(1) If $m = 5$ then $m^{299} = 5^{299} \equiv 283 \pmod{493}$ so the encrypted message is 283. Fast powering algorithm: since $299 = 256 + 32 + 8 + 2 + 1$ we need to compute 5^{2^i} by using $5^{2^i} = (5^{2^{i-1}})^2$ up to $5^{256} \bmod 493$. In modulo 493 we have $5^1 = 5, 5^2 = 25, 5^4 = 132, 5^8 = 169, 5^{16} = 460, 5^{32} = 103, 5^{64} = 256, 5^{128} = 460$, and $5^{256} = 103$. Then,

$$\begin{aligned} 5^{299} &= 5^{256+32+8+2+1} \\ &= 5^{256} \cdot 5^{32} \cdot 5^8 \cdot 5^2 \cdot 5 \\ &= 103 \cdot 103 \cdot 169 \cdot 25 \cdot 5 \\ &\equiv 283 \pmod{493}. \end{aligned}$$

(2) Notice that $\gcd(283, 493) = 1$. Furthermore, $\varphi(493) = 16 \cdot 28 = 448$ and $\gcd(299, 448) = 1$. Therefore we may safely assume that the solution to

$$x^{299} \equiv 283 \pmod{493}$$

is of form 283^d. Then,

$$283^{299d} \equiv 283 \pmod{493} \implies 283^{299d-1} \equiv 1 \pmod{493} \implies \varphi(493) = 448 \mid 299d - 1.$$

Now it remains to solve the congruence relation $299d \equiv 1 \pmod{448}$. "Inspection" suggests $d = 3$ is a solution. Since $\gcd(299, 448) = 1$, this is going to be the only solution between 0 and 447. [Otherwise we would have $448 \mid 299(x' - 3)$ which is clearly impossible.] Hence the decryption exponent $d = 3$.

(3) Here we want to find the number of x's satisfying

$$x \in (\mathbb{Z}/493\mathbb{Z})^* \text{ and } x^{299} \equiv x \pmod{493}.$$

With the conditions above, we may cancel one x on both sides and get

$$x^{298} = 1 \pmod{493} \implies o(x) \mid 298 \text{ in } (\mathbb{Z}/493\mathbb{Z})^*.$$

On the other hand, $x \in (\mathbb{Z}/493\mathbb{Z})^*$ also implies $o(x) \mid \varphi(493) = 448$. Hence $o(x) \mid \gcd(298, 448) = 2$, and thus either $o(x) = 1$ or $o(x) = 2$.

The first case is simple: $o(x) = 1 \implies x = 1$. Indeed $1^{299} \equiv 1 \pmod{493}$.

For the second case, we want to find all solutions to $x^2 \equiv 1 \pmod{493} \implies 17 \cdot 29 \mid (x-1)(x+1)$. If both 17 and 29 divide $x-1$ then $x = 1$, same as above. If both divide $x+1$ then $x = 492$. If one divides $(x-1)$ and the other $(x+1)$ then we either have $x = 86$ or $x = 407$. [This was also a homework problem.]

Hence there are *four* distinct messages that have this property: $1, 86, 407$, and 492.

Solution: Problem 4

(1) To ensure $a^2 \equiv b^2 \pmod{247}$, we just need to make sure $13 \cdot 19 \mid (a-b)(a+b)$. Below is one example:

$$\begin{cases} a-b = 13 \\ a+b = 19 \end{cases} \implies \begin{cases} a = 16 \\ b = 3 \end{cases}$$

Then taking multiples of this pair gives even more pairs: $(a,b) = (32,6), (48,9)$, and $(64,12)$.

(2) No he won't. To succeed, Bob needs to somehow multiply some of the c's and get a product — which we call k — that's congruent to a square, i.e., the product of p's, each raised to some even power.

First look at the powers of p_1. Since all c's have p_1 raised to odd powers, if k existed, it's either the product of two c's or four c's to ensure the even power of p_1. However, $k = c_1c_2c_3c_4$ is impossible because the powers of other p's will be odd this way. Therefore k must be the product of two c's.

Now look at powers of p_2 which should also be even. Since c_4 is the only one with even power, it cannot be part of k. Hence we are now limited to choosing two c's among $\{c_1, c_2, c_3\}$.

Likewise, for powers of p_3, we exclude the possibility of choosing c_3 as it's the only one with even power of p_3 among $\{c_1, c_2, c_3\}$. Hence we are left with $k = c_1c_2$. This won't work either because the power of p_4 is odd, contradicting to $k \equiv$ a square mod N. Therefore Bob won't succeed with these c's.

Solution: Problem 5

Since $|(\mathbb{Z}/p\mathbb{Z})^*| = 2^k$, we want to show that every $a \in (\mathbb{Z}/p\mathbb{Z})^*$ [which guarantees $\gcd(a,p) = 1$] with Legendre symbol $\left(\frac{a}{p}\right) = -1$ has order 2^k. By Euler's Criterion, this means our targets of interest are any $a \in (\mathbb{Z}/p\mathbb{Z})^*$ such that

$$a^{(p-1)/2} = a^{2^{k-1}} \equiv -1 \pmod{p}.$$

This implies $o(a) \nmid 2^{k-1}$. On the other hand, by Fermat's little theorem,

$$a^{p-1} = a^{2^k} \equiv 1 \pmod{p}$$

which implies $o(a) \mid 2^k$. Therefore the only possibility is if $o(a) = 2^k$ itself. Hence $o(a) = \varphi(p)$ and indeed a is a primitive root mod p.

Solution: Problem 6

Let p be a prime of form $3k+2$. Clearly for any multiple of p, $kp \equiv 0 = 0^3 \pmod{p}$ is trivial. Now suppose we pick $x \not\equiv 0 \pmod{p}$. By Fermat's Little Theorem, we have

$$x^{p-1} = x^{3k+1} \equiv 1 \pmod{p}.$$

Squaring both sides and then multiplying by x gives

$$x^{6k+3} \equiv x \pmod{p} \implies x \equiv (x^{2k+1})^3 \pmod{p}, \text{ a cube.}$$

Having shown both cases, we conclude that every integer is a cube mod p.

Solution: Problem 7

First of all, when $a = 1$, the statement $a^N \equiv a \equiv a^{N-\varphi(N)}$ is trivial.

We will now look at the case where $a \neq 1$ is a prime. It follows that, either $\gcd(a, N) = 1$ or N is a multiple of a. For the former, all we need to do is to apply Fermat's little theorem (or maybe just Euler's):

$$a^{\varphi(N)} \equiv 1 \pmod{N} \implies a^{\varphi(N)+[N-\varphi(N)]} = a^N \equiv a^{N-\varphi(N)} \pmod{N}.$$

If N is a multiple of a, then we can write N as $a^i k$ where $a \nmid k$. It follows that $\gcd(a^i, k) = 1$, and so

$$\begin{aligned} N - \varphi(N) &= a^i k - \varphi(a^i k) \\ &= a^i k - \varphi(a^i)\varphi(k) \\ &= a^i k - a^{i-1}(a-1)\varphi(k). \end{aligned}$$

Again, since $\varphi(k) < k$ always holds and k is some nontrvial factor of N that's at least 2, we have

$$N - \varphi(N) > a^i k - a^{i-1}(a-1)k = a^{i-1}k > a^{i-1}.$$

Furthermore, we claim that $a^{i-1} \geqslant i$ for all prime a and positive integer i,

$$a^{i-1} \geqslant 2^{i-1} \geqslant i$$

because $2^{1-1} = 1$ and, for larger i's, the LHS exponentially outgrows the RHS. Also, since $a^i \mid N$ we also have

$a^N \equiv 0 \pmod{a^i}$. Therefore $N - \varphi(N) \geqslant i$ and we have

$$a^{N-\varphi(N)} \equiv 0 \equiv a^N \pmod{a^i}.$$

On the other hand, since we have constructed k to be coprime with a, we get

$$a^{\varphi(k)} \equiv 1 \pmod{k}.$$

Recall that $\varphi(N) = \varphi(a^i)\varphi(k)$ so $\varphi(k) \mid \varphi(N)$, and thus

$$a^{\varphi(N)} \equiv 1 \pmod{k} \implies a^{\varphi(N)+[N-\varphi(N)]} = a^N \equiv a^{N-\varphi(N)} \pmod{k}.$$

Therefore,

$$\begin{cases} a^N \equiv a^{N-\varphi(N)} \pmod{a^i} \\ a^N \equiv a^{N-\varphi(N)} \pmod{k} \end{cases} \implies a^N \equiv a^{N-\varphi(N)} \pmod{a^i k}, \text{ i.e., } \pmod{N}.$$

Now, for the seemingly more complicated case where a can be a composite, we only need to notice that if

$$x^N \equiv x^{N-\varphi(N)} \pmod{N} \text{ and } y^N \equiv y^{N-\varphi(N)} \pmod{N}$$

then so does their product xy, i.e., $(xy)^N \equiv (xy)^{N-\varphi(N)} \pmod{N}$. If a composite $a = \prod {p_i}^{e_i}$ is coprime to N, then all its prime factors, i.e., all the p_i's, are also coprime to N. Then the congruence relation holds for each p_i's, and from what we've shown above, we are able to conclude that $a^N \equiv a^{N-\varphi(N)} \pmod{N}$ as well.