The University of Sydney
School of Mathematics and Statistics

Solutions to Tutorial 9 (Week 11)

MATH2068/2988: Number Theory and Cryptography — Semester 2, 2017

Web Page: http://www.maths.usyd.edu.au/u/UG/IM/MATH2068/
Lecturer: Dzmitry Badziahin

Tutorial Exercises:

1. Find a quadratic polynomial $P(x) = ax^2 + bx + c$, where the coefficients a, b, c belong to $\{0, 1, 2, 3, 4, 5, 6\}$, such that the following all hold:

$$P(2) \equiv 5 \pmod 7,$$
$$P(3) \equiv 4 \pmod 7,$$
$$P(5) \equiv 1 \pmod 7.$$

Solution: The Lagrange Interpolation Formula in modular arithmetic gives

$$P(x) = 5\frac{(x-3)(x-5)}{(2-3)(2-5)} + 4\frac{(x-2)(x-5)}{(3-2)(3-5)} + \frac{(x-2)(x-3)}{(5-2)(5-3)},$$

where each fraction indicates that we multiply the numerator by a mod-7 inverse of the denominator. Since an inverse of $(2-3)(2-5) = 3$ is 5, an inverse of $(3-2)(3-5) = -2$ is 3, and an inverse of $(5-2)(5-3) = 6$ is -1, we get

$$P(x) = 4(x-3)(x-5) - 2(x-2)(x-5) - (x-2)(x-3) \equiv x^2 + x + 6 \pmod 7.$$

So $a = 1$, $b = 1$, $c = 6$ is a solution, in fact the unique solution with $a, b, c \in \{0, 1, 2, 3, 4, 5, 6\}$.

2. Given that 7 is a primitive root modulo 71 (which is prime), find the discrete logarithm $\log_{7,71}(3)$, i.e. the unique $x \in \{0, 1, \cdots, 69\}$ such that $7^x \equiv 3 \pmod{71}$. It is quickest to use the Pohlig–Hellman algorithm, i.e. to find the residues of x modulo the prime factors 2, 5, 7 of 70 and then solve the resulting system of congruences for x. You will need the following congruences mod 71:

$$3^{35} \equiv 1, \qquad 7^{35} \equiv 70,$$
$$3^{14} \equiv 54, \qquad 7^{14} \equiv 54,$$
$$3^{10} \equiv 48, \qquad 7^{10} \equiv 45.$$

Solution: Recall from lectures that, to find the residue r of x modulo q where q is a prime factor of 70, we can raise both sides of the congruence $7^x \equiv 3 \pmod{71}$ to the power $70/q$ and use the fact that $7^{70/q}$ has order q to conclude that

$$(7^{70/q})^r \equiv 3^{70/q} \pmod p.$$

This is a smaller discrete logarithm problem which we can then solve by the naive method of trying all possible values of $r \in \{0, 1, \cdots, q-1\}$. Of course, the reason why this is a sensible approach in the present case is that the prime factors 2, 5, and 7 of 70 are all small.

Applying this with $q = 2$, we have to solve $70^r \equiv 1 \pmod{71}$, and the solution is obviously $r = 0$. So $x \equiv 0 \pmod{2}$.

Applying this with $q = 5$, we have to solve $54^r \equiv 54 \pmod{71}$, and the solution is obviously $r = 1$. So $x \equiv 1 \pmod{5}$.

Applying this with $q = 7$, we have to solve $45^r \equiv 48 \pmod{71}$. After calculating the residues of 45^2, 45^3, 45^4 and $45^5 \pmod{71}$ we find the solution $r = 5$, so $x \equiv 5 \pmod{7}$.

We now have to solve the system of congruences $x \equiv 0 \pmod{2}$, $x \equiv 1 \pmod{5}$, and $x \equiv 5 \pmod{7}$. The general solution is $x \equiv 26 \pmod{70}$, and we conclude that $\log_{7,71}(3) = 26$.

3. 101 is prime, and 2 is a primitive root modulo 101; thus any integer coprime to 101 is congruent modulo 101 to 2^i for some $i \in \{0, 1, \cdots, 99\}$. Find all solutions x of the following congruences which belong to the standard reduced system $\{1, 2, \cdots, 100\}$.

(a) $x^5 \equiv 1 \pmod{101}$

Solution: By a general result from lectures, since 5 divides $\phi(101) = 100$, there are 5 fifth roots of 1 modulo 101. In terms of the primitive root 2, these tenth roots are 2^0, 2^{20}, 2^{40}, 2^{60}, 2^{80} (recall that this is because $(2^i)^5 \equiv 1 \pmod{101}$ if and only if $5i \equiv 0 \pmod{100}$, i.e. i is a multiple of 20). Since $2^{10} = 1024$ is congruent to 14 modulo 101, we have $2^{20} \equiv 196 \equiv 95 \equiv -6 \pmod{101}$. So our 5 solutions can also be described as the residues of the powers of -6. Starting at 1 and repeatedly multiply by -6 and reducing modulo 101, we get the following list of solutions: 1, 95, 36, 87, 84.

(b) $x^5 \equiv 32 \pmod{101}$

Solution: Obviously there are solutions, since $x = 2$ is a solution. Hence there are five solutions, obtained from the known solution 2 by multiplying by the fifth roots of 1, which from the previous question are 1, 95, 36, 87, 84. So the solutions are 2, 89, 72, 73, 67. In terms of the primitive root 2, the solutions are the powers 2^i such that $2^{5i} \equiv 2^5 \pmod{101}$, or equivalently $5i \equiv 5 \pmod{100}$, i.e. $i = 1 + 20\ell$ for $\ell \in \{0, 1, 2, 3, 4\}$.

(c) $x^2 \equiv -1 \pmod{101}$

Solution: Obviously $x = 10$ is a solution, and the other solution must then be $101 - 10 = 91$. In terms of the primitive root 2, the solutions are the powers 2^i such that $2^{2i} \equiv 2^{50} \pmod{101}$, or equivalently $2i \equiv 50 \pmod{100}$, i.e. $i = 25$ or $i = 75$.

(d) $x^{67} \equiv 10 \pmod{101}$

Solution: Since 67 is coprime to $\phi(101) = 100$, there is a unique solution, which we can find as follows. An inverse of 67 modulo 100 is 3, so $(x^{67})^3 =$

$x^{201} \equiv x$ for all x (by Fermat's Little Theorem). So raising both sides of the desired congruence to the power 3 gives $x \equiv 10^3 \equiv 91 \pmod{101}$.

In this case, the primitive root 2 was not needed; but if we had wanted to use it, we could have observed that since $10^2 \equiv -1 \pmod{101}$, the order of 10 modulo 101 is 4, which means that either $10 \equiv 2^{25} \pmod{101}$ or $10 \equiv 2^{75} \pmod{101}$, and a quick calculation shows that in fact $10 \equiv 2^{25} \pmod{101}$. Then the solutions of $x^{67} \equiv 10 \pmod{101}$ are the powers 2^i such that $2^{67i} \equiv 2^{25} \pmod{101}$, or equivalently $67i \equiv 25 \pmod{100}$, leading to $i = 75$ and $x = 91$ as before.

(e) $x^6 \equiv 4 \pmod{101}$

Solution: In terms of the primitive root 2, the solutions are the powers 2^i such that $2^{6i} \equiv 2^2 \pmod{101}$, or equivalently $6i \equiv 2 \pmod{100}$, i.e. $3i \equiv 1 \pmod{50}$, leading to $i = 17$ and $i = 67$. The residue of 2^{17} modulo 101 is 75; the residue of $2^{67} = 2^{17}2^{50}$ modulo 101 is then $101 - 75 = 26$.

(f) $x^2 \equiv 2 \pmod{101}$

Solution: There are no solutions: since 2 is a primitive root mod 101, it cannot be a quadratic residue. Explicitly, in terms of the primitive root 2, the solutions are the powers 2^i such that $2^{2i} \equiv 2^1 \pmod{101}$, or equivalently $2i \equiv 1 \pmod{100}$, which is impossible.

***4.** From the point of view of the Discrete Logarithm Problem, the easiest moduli m to handle are those where $\phi(m)$ has only small prime factors.

(a) For which positive integers m is $\phi(m)$ a power of 2?

Solution: If m has prime factorization $p_1^{k_1} \cdots p_r^{k_r}$ for distinct primes $p_1, \cdots, p_r$ and positive integers $k_1, \cdots, k_r$, then $\phi(m) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r})$, so $\phi(m)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i. Now $\phi(p^k) = p^{k-1}(p-1)$, and there are only two ways this can equal a power of 2: either $p = 2$ and k is arbitrary, or $p = 2^a + 1$ for some positive integer a and $k = 1$. In the latter case, $a = 2^i$ must itself be a power of 2, as seen in Q8 of Tutorial 2; that is, $p = 2^{2^i} + 1$ must be a Fermat prime. So the answer is that m must be a power of 2 times a product (possibly empty) of distinct Fermat primes. The only known Fermat primes are $3, 5, 17, 257, 65537$.

(b) For which positive integers m is $\phi(m)$ a power of 3?

Solution: This is a sort of trick question: $\phi(m)$ is even unless $m \in \{1, 2\}$, as is easily seen from the formula in terms of prime factorization (or from the fact that the numbers coprime to $m > 2$ occur in pairs $\{a, m - a\}$). So the answer is just $m = 1$ or $m = 2$, for which $\phi(m) = 1 = 3^0$.

(c) For which positive integers m is $\phi(m)$ twice a power of 3?

Solution: Certainly $m = 4$, $m = 3^k$ and $m = 2 \times 3^k$ for any positive integer k have this property. If m is not of any of these forms, then from the formula for $\phi(m)$ in terms of the prime factorization of m, we see that either $m = p$ or $m = 2p$ where p is a prime of the form $2 \times 3^a + 1$ for some positive integer a. (The list of such primes begins $3, 7, 19, 163, 487, \ldots$. They appear not to have a special name, and it is not known whether there are infinitely many of them.)

5. Suppose that for security you want to split the knowledge of a secret positive integer c between four people, P_1, P_2, P_3 and P_4. You choose a prime p larger than c and random positive integers a and b less than p, and tell person P_i the prime p and the number r_i which is the residue of $ai^2 + bi + c$ modulo p. Suppose that each of the four people knows the procedure that you followed, without knowing a, b, c.

(a) How many people need to combine their information to be able to determine c, and how would they do it?

Solution: Since we are dealing with a polynomial of degree 2, namely $f(x) = ax^2 + bx + c$, with three undetermined coefficients, three values are required to determine it. If P_i, P_j and P_k (for $i, j, k \in \{1, 2, 3, 4\}$ distinct) combine their information, then they know that $f(i) \equiv r_i \pmod{p}$, $f(j) \equiv r_j \pmod{p}$ and $f(k) \equiv r_k \pmod{p}$, and they can find $f(x)$ (and hence $f(0) = c$) using the Lagrange Interpolation Formula as in Q1. Note that the information held by two people P_i and P_j is not enough to determine c, because one could find a polynomial $f(x)$ of degree ≤ 2 satisfying $f(i) \equiv r_i \pmod{p}$, $f(j) \equiv r_j \pmod{p}$ and $f(0) \equiv c \pmod{p}$ for any value of c whatsoever.

**(b) To what extent would it be less secure to tell each person P_i the actual value n_i of $ai^2 + bi + c$, rather than its residue r_i modulo a chosen prime p?

Solution: If person P_i was told $n_i = ai^2 + bi + c$, then individually they would know only a bit more than in the previous case. Person P_i would know that $a < n_i/i^2$, $b < n_i/i$, $c < n_i$ (which could be more useful than it was in the previous system to know that $a, b, c < p$); moreover, P_2, P_3 and P_4 would know the congruence class of c modulo 2, 3 and 4 respectively. A more significant difference would come when two people P_i and P_j combined their information, because they would then be able to compute

$$\frac{n_i - n_j}{i - j} = \frac{(ai^2 + bi + c) - (aj^2 + bj + c)}{i - j} = a(i + j) + b,$$

and hence also

$$(i + j)n_i - i^2\frac{n_i - n_j}{i - j} = (i + j)(ai^2 + bi + c) - i^2(a(i + j) + b) = bij + c(i + j).$$

These pieces of knowledge would give them ways of cutting down the possibilities for the positive integers a, b, c. For example, write the first piece of knowledge as $a(i + j) + b = M$, where i, j, M are known. One can deduce from this that b has the same residue as M modulo $i + j$, say r, so b must be of the form $q(i + j) + r$ where q is an integer satisfying $0 \leq q < \frac{M-r}{i+j}$. Now we can write the second piece of knowledge as $(q(i + j) + r)ij + c(i + j) = N$ where i, j, r, N are known and q is bounded as above; this rearranges to give $c = \frac{N-rij}{i+j} - qij$, from which one can deduce the congruence class of c modulo ij and the bounds

$$\frac{N - Mij}{i + j} < c \leq \frac{N - rij}{i + j}.$$

This leaves about $\frac{M-r}{ij(i+j)}$ possibilities for c. Depending on the values of n_i and n_j, this may or may not be noteworthy progress towards finding c, but

at least to this extent, the system of disclosing the actual values n_i is less secure than the previous system of disclosing their residues mod p, where two people combined could deduce practically nothing.

Extra Exercises:

6. Find $a, b, c \in \{0, 1, \ldots, 18\}$ such that the polynomial $f(x) = ax^2 + bx + c$ satisfies $f(3) \equiv 11$, $f(7) \equiv 2$ and $f(16) \equiv 9 \pmod{19}$.

Solution: Let $f_1(x) = (x-7)(x-16)$, $f_2(x) = (x-3)(x-16)$, $f_3(x) = (x-3)(x-7)$ be the numerators of the fractions in the Lagrange Interpolation Formula. Then $f_1(x) \equiv x^2 - 4x - 2 \pmod{19}$, $f_2(x) \equiv x^2 - 9 \pmod{19}$ and $f_3(x) \equiv x^2 + 9x + 2 \pmod{19}$. The corresponding denominators are:

$$\begin{aligned} f_1(3) &\equiv 9 - 12 - 2 \equiv -5 \\ f_2(7) &\equiv 11 - 9 \equiv 2 \\ f_3(16) &\equiv 9 - 27 + 2 \equiv 3 \end{aligned}$$

and inverses of these numbers mod 19 are -4, 10 and -6. So the polynomial we want is

$$11(-4x^2 + 16x + 8) + 2(10x^2 - 90) + 9(-6x^2 - 54x - 12),$$

congruent to $17x^2 + 13x + 9 \pmod{19}$. So the answer is $a = 17$, $b = 13$ and $c = 9$.

7. Given that 3 is a primitive root modulo 31, use the Pohlig–Hellman algorithm to find the discrete logarithm $\log_{3,31}(10)$, i.e. the unique $x \in \{0, 1, \cdots, 29\}$ such that $3^x \equiv 10 \pmod{31}$.

Solution: In this algorithm, we find the residues of x modulo 2, 3 and 5 separately and then solve the resulting system of congruences. See the solution to Q2 for details of the method.

Since $3^{15} \equiv -1 \pmod{31}$ and $10^{15} \equiv 1 \pmod{31}$, the smallest solution of $(3^{15})^r \equiv 10^{15} \pmod{31}$ is $r = 0$. So $x \equiv 0 \pmod{2}$.

Since $3^{10} \equiv 25 \pmod{31}$ and $10^{10} \equiv 5 \pmod{31}$, the smallest solution of $(3^{10})^r \equiv 10^{10} \pmod{31}$ is $r = 2$. So $x \equiv 2 \pmod{3}$.

Since $3^6 \equiv 16 \pmod{31}$ and $10^6 \equiv 2 \pmod{31}$, the smallest solution of $(3^6)^r \equiv 10^6 \pmod{31}$ is $r = 4$. So $x \equiv 4 \pmod{5}$.

Solving simultaneously the congruences $x \equiv 0 \pmod{2}$, $x \equiv 2 \pmod{3}$ and $x \equiv 4 \pmod{5}$, we find that $\log_{3,31}(10) = 14$.

8. Given that 5 is a primitive root modulo 257 (which is prime), find the discrete logarithm $\log_{5,257}(2)$, i.e. the unique $x \in \{0, 1, \cdots, 255\}$ satisfying $5^x \equiv 2 \pmod{257}$. (Hint: use the fact that $2^8 \equiv -1 \pmod{257}$ to cut down the possibilities for x.)

Solution: Since $2^8 \equiv -1 \pmod{257}$, we know that $5^{8x} \equiv -1 \equiv 5^{128} \pmod{257}$, so $8x \equiv 128 \pmod{256}$, which implies that $x \equiv 16 \pmod{32}$, meaning that we have only eight possibilities for x, namely $16, 48, 80, 112, \cdots, 240$. By successive

squaring we can quickly find that $5^{16} \equiv -32 \pmod{257}$ and $5^{32} \equiv -4 \pmod{257}$, from which we get $5^{48} \equiv 128 \pmod{257}$ and $5^{80} \equiv 2 \pmod{257}$. So $\log_{5,257}(2) = 80$.

***9.** Given that 2 is a primitive root modulo 81 (that is, $\mathrm{ord}_{81}(2) = \phi(81) = 54$), find $\log_{2,81}(5)$, i.e. the unique $x \in \{0, 1, \cdots, 53\}$ satisfying $2^x \equiv 5 \pmod{81}$. (Hint: an efficient method is to solve the congruence $2^x \equiv 5$ modulo 3, then modulo 9, then modulo 27, then modulo 81.)

Solution: The congruence $2^x \equiv 5 \pmod{3}$ has solution $x \equiv 1 \pmod{2}$. So in solving the stronger congruence $2^x \equiv 5 \pmod{9}$ we need only try odd values of x (and we know there must be a solution with x less than $\mathrm{ord}_9(2) = \phi(9) = 6$); this quickly leads to the solution $x \equiv 5 \pmod{6}$. Then in solving the stronger congruence $2^x \equiv 5 \pmod{27}$ we need only try values of x satisfying $x \equiv 5 \pmod{6}$, and $x = 5$ already works, so the solution is $x \equiv 5 \pmod{18}$. Finally, to solve the congruence $2^x \equiv 5 \pmod{81}$ we need only try values of x satisfying $x \equiv 5 \pmod{18}$; this quickly leads to the solution that $\log_{2,81}(5) = 23$.