The University of Sydney
School of Mathematics and Statistics

Solutions to Tutorial 8 (Week 10)

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

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

In the Diffie–Hellman key exchange protocol, Alice posts a public key (p, b, k) where p is a prime, b is a nonzero residue mod p, and k is the residue of b^x mod p for some nonnegative integer x, which is Alice's private key. Bob responds with c, the residue of b^y mod p where y is a nonnegative integer which is Bob's private key. Then Alice and Bob have a shared secret number s, the residue of b^{xy} mod p, since $s \equiv k^y \equiv c^x \pmod{p}$.

In the Elgamal cryptosystem, s is used as a scrambling factor to multiply residues mod p. After Alice has posted her public key (p, b, k), Bob chooses a private key y, computes the residue c of b^y mod p, and also computes the shared secret s as the residue of k^y mod p. Having encoded his message as a residue M mod p (or, for a longer message, a sequence $[M_1, \cdots, M_\ell]$ of such residues), he encrypts it by replacing M with the residue M' of sM mod p (or by replacing each M_i with the residue M_i' of sM_i mod p). The ciphertext he sends is $\langle c, M' \rangle$ (or $\langle c, [M_1', \cdots, M_\ell'] \rangle$). Alice can compute s as the residue of c^x mod p, and can thus decrypt the message by multiplying by the inverse of s.

Tutorial Exercises:

1. This question illustrates the Diffie–Hellman key exchange protocol with small (and hence unrealistic) numbers. Suppose that Alice posts the public key $(31, 3, 13)$.

(a) If you are Bob, and choose your private key to be 4, what should you send to Alice, and what is the shared secret number that results?

Solution: You should send to Alice the residue of 3^4 mod 31, which is 19. The secret that you and Alice then share is the residue of 13^4 mod 31, which is 10.

(b) Solve $3^x \equiv 13 \pmod{31}$ to find Alice's private key.

Solution: Since the numbers involved are so small, it is possible just to find the residues of the powers 3^i mod 31 by successively multiplying by 3 and reducing mod 31:

i	0	1	2	3	4	5	6	7	8	9	10	11
3^i	1	3	9	27	19	26	16	17	20	29	25	13

We conclude that Alice's private key x is 11. In other words, $\log_{3,31}(13) = 11$. (Note that any value of x congruent to 11 modulo 30 would also satisfy $3^x \equiv 13 \pmod{31}$ and so could also be considered to be Alice's private key.)

(c) Now suppose you are an eavesdropper who has worked out Alice's private key as in the previous part. If you overhear that Bob's message to Alice is 5, what is their shared (supposedly) secret number?

Solution: Since Alice's private key is 11, the shared secret is the residue of 5^{11} mod 31, which is 25 (easy to calculate, because $5^3 \equiv 1 \pmod{31}$).

2. Amy, a user of the Elgamal cryptosystem, has posted the public key $(47, 5, 2)$.

(a) Encrypt the message $[12, 26, 33]$ to send to Amy, choosing 7 as your private key.

Solution: The choice of 7 as our private key means that the scrambling factor is the residue of $2^7 = 128$ modulo 47, which is 34. We must multiply each term of the plaintext by this scrambling factor, reducing modulo 47: this gives $[32, 38, 41]$ (for instance, $12 \times 34 = 408 \equiv 32 \pmod{47}$). We also compute that $5^7 \equiv 11 \pmod{47}$. This residue 11 is the extra information that we send Amy to allow her to work out the scrambling factor. So the ciphertext we send is $\langle 11, [32, 38, 41] \rangle$.

(b) Now suppose you are an eavesdropper who wants to decrypt messages sent to Amy. You calculate that $5^{18} \equiv 2 \pmod{47}$, which means that 18 is Amy's private key. Use this knowledge to decrypt the ciphertext $\langle 8, [17, 29, 35] \rangle$.

Solution: The scrambling factor used to encrypt this message must have been the residue of 8^{18} modulo 47, which is 21 because $8^{18} = 2^{54} \equiv 2^8 \equiv 21 \pmod{47}$. To decrypt it, we need the inverse of 21 modulo 47, which is easily seen to be 9. Then we must multiply each term of $[17, 29, 35]$ by 9 and reduce modulo 47, giving $[12, 26, 33]$. Notice that this is the same message we encrypted in the previous part, but the two ciphertexts were not the same: this is because encrypting a message requires choosing a private key. The ciphertext $\langle 8, [17, 29, 35] \rangle$ results from choosing 8 as the private key, instead of 7 as in the previous part.

3. Let p be a prime and $b \in \{1, \cdots, p-1\}$ a primitive root modulo p; recall that this means that $\mathrm{ord}_p(b) = p - 1$. For any $a \in \{1, \cdots, p-1\}$, there is a unique $i \in \{0, 1, \cdots, p-2\}$ such that $b^i \equiv a \pmod{p}$; we call this i the discrete logarithm of a to the base b modulo p, written $\log_{b,p}(a)$. This exercise shows that some of the usual logarithm laws hold for discrete logarithms, if interpreted appropriately.

(a) Suppose $a_1, a_2, a_3 \in \{1, \cdots, p-1\}$ satisfy $a_3 \equiv a_1 a_2 \pmod{p}$. Show that

$$\log_{b,p}(a_3) \equiv \log_{b,p}(a_1) + \log_{b,p}(a_2) \pmod{p-1}.$$

Solution: Working modulo p, we have

$$b^{\log_{b,p}(a_3)} \equiv a_3 \equiv a_1 a_2 \equiv b^{\log_{b,p}(a_1)} b^{\log_{b,p}(a_2)} = b^{\log_{b,p}(a_1) + \log_{b,p}(a_2)}.$$

This implies that $\log_{b,p}(a_3)$ is congruent to $\log_{b,p}(a_1) + \log_{b,p}(a_2)$ modulo $\mathrm{ord}_p(b)$, which is $p - 1$.

(b) Suppose $a_1, a_2 \in \{1, \cdots, p-1\}$ are inverse to each other mod p. Show that

$$\log_{b,p}(a_2) \equiv -\log_{b,p}(a_1) \pmod{p-1}.$$

Solution: We have $a_1 a_2 \equiv 1 \pmod{p}$, so we can set $a_3 = 1$ in the result of the previous part. It is clear from the definition that $\log_{b,p}(1) = 0$, so we deduce that $0 \equiv \log_{b,p}(a_1) + \log_{b,p}(a_2) \pmod{p-1}$, which rearranges to the desired congruence.

(c) Suppose $b' \in \{1, \cdots, p-1\}$ is another primitive root modulo p. Show that for any $a \in \{1, \cdots, p-1\}$ we have

$$\log_{b,p}(a) \equiv \log_{b,p}(b') \log_{b',p}(a) \pmod{p-1}.$$

Solution: Working modulo p, we have

$$b^{\log_{b,p}(b') \log_{b',p}(a)} = \left(b^{\log_{b,p}(b')}\right)^{\log_{b',p}(a)} \equiv (b')^{\log_{b',p}(a)} \equiv a \equiv b^{\log_{b,p}(a)}.$$

This implies that $\log_{b,p}(b') \log_{b',p}(a) \equiv \log_{b,p}(a)$ modulo $\text{ord}_p(b) = p - 1$.

4. Show that 3 is a primitive root modulo 19, and make a table giving the values of $\log_{3,19}(a)$ for all nonzero residues a modulo 19. Which other nonzero residues are primitive roots?

Solution: Starting with 1, we repeatedly multiply by 3 and reduce modulo 19, obtaining the following table of powers of 3 mod 19:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3^i	1	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1

So the order of 3 modulo 19 is indeed 18, showing that 3 is a primitive root mod 19. As predicted by the general results in lectures, every nonzero residue a mod 19 is the residue of 3^i for a unique i with $0 \leq i < 18$, and it is this unique i that is defined to be $\log_{3,19}(a)$. So we get the desired table of logarithms by switching the two rows of the table of powers:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{3,19}(a)$	0	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

By a result from lectures, the number of nonzero residues mod 19 which are primitive roots is $\phi(18) = \phi(2 \times 3^2) = 6$. By another result we know that, given one primitive root b (such as $b = 3$), the complete set of primitive roots can be found by taking the residues of b^k where $1 \leq k \leq 17$ and $\gcd(k, 18) = 1$. (Recall the reason for this: if $d = \gcd(k, 18) \neq 1$, then $(b^k)^{18/d} \equiv 1 \pmod{p}$, so $\text{ord}_{19}(b^k)$ is strictly less than 18.) So the primitive roots are the residues of 3^1, 3^5, 3^7, 3^{11}, 3^{13} and 3^{17} mod 19, namely 3, 15, 2, 10, 14, 13.

5. If m is any positive integer and $b \in \mathbb{Z}$, we say that b is a primitive root modulo m if $\gcd(b, m) = 1$ and $\text{ord}_m(b) = \phi(m)$. It was proved in lectures that such primitive roots always exist when m is prime; this question investigates the case where $m = p^k$ for p a prime and $k \geq 2$.

*(a) It is easy to see that 3 is a primitive root modulo 4. However, there is no primitive root modulo 8, because 3, 5, and 7 all have order 2 modulo 8. Deduce that there is no primitive root modulo 2^k where $k \geq 4$.

Solution: Suppose for a contradiction that b is a primitive root modulo 2^k for $k \geq 4$. Then b is odd and $\text{ord}_{2^k}(b) = 2^{k-1}$; this implies that $\{b^0, b^1, \cdots, b^{2^{k-1}-1}\}$ is a reduced system modulo 2^k, which means that every odd integer is congruent modulo 2^k to some power of b. Then, since $8 \mid 2^k$, we can deduce that every odd integer is congruent modulo 8 to some power of b. But this implies that b is a primitive root modulo 8, which we know is impossible.

**(b) Show that if $m = p^k$ where p is an odd prime and $k \geq 2$, then there is a primitive root modulo m. (Hint: show that there is a primitive root b modulo p which satisfies $b^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ for all $k \geq 2$.)

Solution: Let b be a primitive root modulo p; we certainly have $b^{p-1} \equiv 1 \pmod{p}$. If $b^{p-1} \equiv 1 \pmod{p^2}$, then replace b with $b + p$ (which is clearly also a primitive root modulo p): by the binomial theorem, we have

$$(b+p)^{p-1} \equiv b^{p-1} + (p-1)p \equiv 1 - p \not\equiv 1 \pmod{p^2}.$$

So we can assume that b is a primitive root modulo p satisfying $b^{p-1} \not\equiv 1 \pmod{p^2}$. We claim that this implies that $b^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ for all $k \geq 2$. We will prove this claim by induction on k: since we know the $k = 2$ base case, we need only show that the statement for k implies the statement for $k + 1$. Since $b^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$ by the Euler–Fermat Theorem, our assumption means that

$$b^{p^{k-2}(p-1)} = 1 + ap^{k-1}$$

for some integer a such that $\gcd(a, p) = 1$. By the binomial theorem, we deduce that

$$b^{p^{k-1}(p-1)} = (1+ap^{k-1})^p \equiv 1+ap^k+a^2\binom{p}{2}p^{2k-2} \equiv 1+ap^k \not\equiv 1 \pmod{p^{k+1}},$$

as required. Here we are using the assumption that p is odd to guarantee that $\binom{p}{2}$ is a multiple of p, which is needed in the $k = 2$ case of this argument to ensure that $\binom{p}{2}p^{2k-2}$ is a multiple of p^{k+1}.

Now to show that b is a primitive root modulo p^k for any $k \geq 2$, we must show that $\mathrm{ord}_{p^k}(b) = p^{k-1}(p-1)$; we know by the Euler–Fermat Theorem that $\mathrm{ord}_{p^k}(b)$ divides $p^{k-1}(p-1)$. Since the congruence $b^j \equiv 1 \pmod{p^k}$ implies that $b^j \equiv 1 \pmod{p}$ which in turn implies that j is a multiple of $\mathrm{ord}_p(b) = p-1$, we also know that $\mathrm{ord}_{p^k}(b)$ is a multiple of $p-1$, so we must have $\mathrm{ord}_{p^k}(b) = p^i(p-1)$ for some nonnegative integer $i \leq k-1$. On the other hand, the fact that $b^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ shows that $\mathrm{ord}_{p^k}(b)$ does not divide $p^{k-2}(p-1)$, so we must have $i = k-1$ as required.

Extra Exercises:

6. Your Elgamal public key is $(3937201, 158, 7111)$, your private key being 3. You receive the ciphertext $\langle 61320, 62799\rangle$. Decrypt it to find the original message.

Solution: (Note that the values 158 and 7111 are not actually used in decryption.) The first task is to compute the scrambling factor, which is the residue of 61320^3 modulo 3937201. We find that $61320^2 = 3760142400$, and the residue of this mod 3937201 is 115445. So

$$61320^3 \equiv 115445 \times 61320 = 70790874000,$$

and the residue of this mod 3937201 is 2. So to find the original message x we must solve $2x \equiv 62799 \pmod{3937201}$. The answer is

$$\tfrac{1}{2}(62799 + 3937201) = \tfrac{1}{2}(4000000) = 2000000.$$

***7.** Suppose that m has prime factorization $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where $p_1, p_2, \cdots, p_r$ are distinct primes and $k_1, k_2, \cdots, k_r \in \mathbb{Z}^+$. Let $b \in \mathbb{Z}$ be such that $\gcd(b, m) = 1$.

(a) Show that $\mathrm{ord}_m(b)$ is the least common multiple of $\mathrm{ord}_{p_1^{k_1}}(b), \cdots, \mathrm{ord}_{p_r^{k_r}}(b)$.

Solution: Note that the orders $\mathrm{ord}_{p_i^{k_i}}(b)$ make sense, because the assumption that $\gcd(b, m) = 1$ is equivalent to saying that $\gcd(b, p_i^{k_i}) = 1$ for all i. If j is a positive integer, we have $b^j \equiv 1 \pmod{m}$ if and only if $b^j \equiv 1 \pmod{p_i^{k_i}}$ for all i. (The "only if" direction follows from the general properties of congruences; the "if" direction follows from the Chinese Remainder Theorem.) Since $b^j \equiv 1 \pmod{p_i^{k_i}}$ is equivalent to saying that j is a multiple of $\mathrm{ord}_{p_i^{k_i}}(b)$, we conclude that $\mathrm{ord}_m(b)$ is the smallest positive integer j which is a multiple of $\mathrm{ord}_{p_i^{k_i}}(b)$ for all i, as claimed.

(b) Hence show that b is a primitive root modulo m if and only if the following two conditions hold: (i) b is a primitive root modulo $p_i^{k_i}$ for all $i \in \{1, \cdots, r\}$, and (ii) the numbers $\phi(p_1^{k_1}), \cdots, \phi(p_r^{k_r})$ are pairwise coprime.

Solution: By the previous part, b is a primitive root modulo m if and only if the least common multiple of the numbers $\mathrm{ord}_{p_1^{k_1}}(b), \cdots, \mathrm{ord}_{p_r^{k_r}}(b)$ equals $\phi(m) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r})$. We also know that each $\mathrm{ord}_{p_i^{k_i}}(b)$ divides $\phi(p_i^{k_i})$ by the Euler–Fermat Theorem. If there is some i such that b is not a primitive root modulo $p_i^{k_i}$, or in other words $\mathrm{ord}_{p_i^{k_i}}(b) < \phi(p_i^{k_i})$, then we can create a common multiple of the numbers $\mathrm{ord}_{p_1^{k_1}}(b), \cdots, \mathrm{ord}_{p_r^{k_r}}(b)$ which is strictly smaller than $\phi(p_1^{k_1}) \cdots \phi(p_r^{k_r})$, by replacing the factor $\phi(p_i^{k_i})$ with $\mathrm{ord}_{p_i^{k_i}}(b)$. Similarly, if $d > 1$ divides both $\phi(p_i^{k_i})$ and $\phi(p_j^{k_j})$ for some $i \neq j$, then we can create a common multiple of the numbers $\mathrm{ord}_{p_1^{k_1}}(b), \cdots, \mathrm{ord}_{p_r^{k_r}}(b)$ which is strictly smaller than $\phi(p_1^{k_1}) \cdots \phi(p_r^{k_r})$, by dividing the latter by d. This shows that if b is a primitive root modulo m then the two stated conditions (i) and (ii) must hold. Conversely, if (i) and (ii) hold then the least common multiple of the numbers $\mathrm{ord}_{p_1^{k_1}}(b) = \phi(p_1^{k_1}), \cdots, \mathrm{ord}_{p_r^{k_r}}(b) = \phi(p_r^{k_r})$ is indeed their product $\phi(m)$.

(c) Combine this with Q5 to determine which moduli m have primitive roots.

Solution: If p is prime and $k \geq 1$, then $\phi(p^k) = p^{k-1}(p-1)$ is always even unless $p = 2$ and $k = 1$. So if m has more than one odd prime factor, or if m contains in its prime factorization both an odd prime factor and a power of 2 larger than 2^1, then more than one of the numbers $\phi(p_1^{k_1}), \cdots, \phi(p_r^{k_r})$ is even, making it impossible for condition (ii) of the previous part to be satisfied. We can conclude that if a primitive root exists modulo m, then m is either a power of a prime or twice a power of an odd prime. By Q5, all prime powers have primitive roots except for 2^k where $k \geq 3$. If $m = 2p^k$ where p is an odd prime, then by Q5 there is some primitive root b modulo p^k; adding the odd number p^k to b if necessary, we can assume that b is odd and hence coprime to $2p^k$, and then b is a primitive root modulo $2p^k$ by the result of part (b). So the complete list of moduli m which have primitive roots is as follows: 1, 2, 4, p^k and $2p^k$ where p is any odd prime and $k \in \mathbb{Z}^+$.