THE UNIVERSITY OF SYDNEY
SCHOOL OF MATHEMATICS AND STATISTICS

Solutions to Tutorial 6 (Week 7)

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. This question illustrates the principles of the RSA cryptosystem with small (and hence unrealistic) numbers. Suppose that an RSA user has a public key of $(33, 3)$.

(a) Encrypt the message $[5, 30, 7]$.

Solution: In the public key of $(33, 3)$, the first number is the modulus and the second number is the encryption exponent. So we encrypt each 'letter' of the message by raising it to the power 3 and then finding the residue modulo 33. Working mod 33 throughout, we have:

$$\begin{aligned} 5^3 &= 125 \equiv 26, \\ 30^3 &\equiv (-3)^3 = -27 \equiv 6, \\ 7^3 &= 343 \equiv 13. \end{aligned}$$

So the encrypted message is $[26, 6, 13]$.

(b) Use the prime factorization of 33 to find $\phi(33)$ and hence determine the private decryption exponent d.

Solution: Since 33 has prime factorization 3×11, $\phi(33) = 2 \times 10 = 20$. So the decryption exponent d is the inverse of 3 modulo 20, which is 7 (for computational convenience, we take the standard representative 7 of the inverse congruence class, rather than 27 say).

(c) Hence decrypt the message $[2, 4, 6]$.

Solution: We decrypt by raising each letter to the power 7 (the decryption exponent found in the previous part) and using the same modulus 33 again. Working mod 33 throughout, we have

$$\begin{aligned} &2^7 = 128 \equiv 29, \\ &4^7 = 2^{14} = 32^2 \times 16 \equiv (-1)^2 \times 16 = 16, \\ &6^7 \equiv 30, \end{aligned}$$

where the last congruence is guaranteed because we already found that 6 is the encryption of 30. So the decrypted message is $[29, 16, 30]$.

2. The number $n = 127349$ is the product of two different primes p and q. But, as this question will show, it would be a bad modulus for the RSA cryptosystem.

(a) Suppose that a website posts the pair (n, e) as its public RSA key, where $n = 127349$ and $e = 5$. If someone wants to send the (single-letter) message 100 to the website using this cryptosystem, what should their ciphertext be?

Solution: The ciphertext is the residue modulo 127349 of $100^5 = 10^{10}$, which is 47124.

(b) Now suppose you are an eavesdropper and want to be able to decrypt messages sent to the website. Apply Fermat's factorization method to the number n to find p and q, and hence find $\phi(n)$.

Solution: The first integer larger than $\sqrt{n}$ is 357, and we find that

$$357^2 - n = 100 = 10^2,$$

so $n = 357^2 - 10^2 = 347 \times 367$. Hence $p = 347$ and $q = 367$ (or the other way around, it makes no difference – it is easy to check by trial division that these two numbers are indeed prime). Hence

$$\phi(n) = (p-1)(q-1) = 346 \times 366 = 126636.$$

(c) Find the private decryption exponent d for this cryptosystem.

Solution: In an RSA cryptosystem with public key (n, e), the decryption exponent d is the inverse of e modulo $\phi(n)$. So we need to find the inverse of 5 modulo 126636. We could use the extended Euclidean algorithm, but it is easier to just find a small multiple of 126636 that is one less than a multiple of 5; we need the final digit to be 4, so we consider

$$126636 \times 4 = 506544 = 5 \times 101309 - 1,$$

showing that the decryption exponent d is 101309.

3. The number $n = 35203807$ is the product of two different primes p and q. Given that $\phi(n) = 35191440$, find p and q.

Solution: We have $\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$. Thus $p + q = n - \phi(n) + 1 = 12368$. We now know both the sum and the product of p and q, which is enough information to determine p and q (strictly speaking, it is enough information to determine the set $\{p, q\}$, because the question did not give any way of specifying which of the two primes is p and which is q).

One way to phrase this is as follows: p and q are the roots of the quadratic polynomial

$$x^2 - (p+q)x + pq = x^2 - 12368x + 35203807.$$

We can use the quadratic formula to find these roots. The discriminant is

$$12368^2 - 4 \times 35203807 = 12152196 = 3486^2,$$

so the roots are

$$\frac{12368 + 3486}{2} = 7927 \quad \text{and} \quad \frac{12368 - 3486}{2} = 4441.$$

*4. Using RSA moduli as small as those in the above questions would be insecure enough, but what would be even worse would be using a public key (n, e) for which the decryption exponent d was *equal* to the encryption exponent e. This happens when e is self-inverse modulo $\phi(n)$, i.e. $e^2 \equiv 1 \pmod{\phi(n)}$.

(a) Show that if $n = 35$, every possible choice of encryption exponent e has this property.

Solution: We have $\phi(35) = (5-1)(7-1) = 24$. We want to show that every positive integer coprime to 24 is self-inverse modulo 24. It is enough to check the elements of the standard reduced system modulo 24, namely $1, 5, 7, 11, 13, 17, 19, 23$. Each of these is indeed self-inverse modulo 24:

$$1^2 = 1, \quad 5^2 = 25 \equiv 1, \quad 7^2 = 49 \equiv 1, \quad 11^2 = 121 \equiv 1,$$

and the other four congruence classes are the negatives of these, so they also square to 1 modulo 24.

(b) Suppose that n is a product of distinct odd primes p and q. Show that there is a solution of $e^2 \equiv 1 \pmod{\phi(n)}$ which is not one of the obvious solutions $e \equiv \pm 1 \pmod{\phi(n)}$.

Solution: We have $\phi(n) = (p-1)(q-1)$. Since each of $p-1$ and $q-1$ is even, $\phi(n)$ is divisible by 4; also, $\phi(n)$ is at least $(3-1)(5-1) = 8$. We are trying to find some e coprime to $\phi(n)$ which squares to 1 modulo $\phi(n)$, and we may as well look in the standard reduced system, i.e. consider only integers e between 1 and $\phi(n) - 1$. The question rules out the extreme cases $e = 1$ and $e = \phi(n) - 1$, so it is somewhat natural to try looking in the middle of the range instead.

Obviously we can't take $e = \frac{\phi(n)}{2}$, since that is not coprime to $\phi(n)$; indeed, it divides $\phi(n)$. Instead, let $e = \frac{\phi(n)}{2} - 1$. (Since $\phi(n) > 4$, we certainly have $1 < e < \phi(n) - 1$, so indeed $e \not\equiv \pm 1 \pmod{\phi(n)}$.) We know that $\frac{\phi(n)}{2}$ is even, so e is odd; it must be coprime to $\phi(n)$, because any common factor of e and $\phi(n)$ would also have to divide $\phi(n) - 2e = 2$. Moreover, we can calculate

$$e^2 - 1 = (e-1)(e+1) = \left(\frac{\phi(n)}{2} - 2\right)\left(\frac{\phi(n)}{2}\right) = \left(\frac{\phi(n)}{4} - 1\right)\phi(n),$$

which is an integer multiple of $\phi(n)$, so $e^2 \equiv 1 \pmod{\phi(n)}$ as desired.

**5. The Möbius Inversion Formula tells us that, if f and F are two functions on the positive integers such that

$$F(n) = \sum_{d|n} f(d) \quad \text{for all } n \in \mathbb{Z}^+,$$

then we have

$$f(n) = \sum_{d|n} \mu(n/d)\, F(d) \quad \text{for all } n \in \mathbb{Z}^+.$$

Use this to find a formula for the number $B(n)$ of strings of n bits (each bit being either 0 or 1) which are *aperiodic*, meaning that there is no proper divisor d of

n such that the string is periodic with period d. (For example, when $n = 4$, the string 0110 is aperiodic, but 0101 is not since it has period 2.)

Solution: Let n be any positive integer. There are 2^n strings of n bits in total, and each one is either aperiodic or periodic with period d for some proper divisor d of n. If we agree that the period of a periodic string means the *minimum* d such that the string repeats every d places, then each periodic string has a uniquely defined period. To write down a string of n bits which is periodic with period d, we just need to write down any aperiodic string of d bits and repeat it n/d times, so the number of such strings is $B(d)$. We conclude from this that

$$\sum_{d|n} B(d) = 2^n.$$

Applying the Möbius Inversion Formula, we obtain the desired formula for $B(n)$:

$$B(n) = \sum_{d|n} \mu(n/d)\, 2^d.$$

For example, $B(6) = \mu(6)\, 2^1 + \mu(3)\, 2^2 + \mu(2)\, 2^3 + \mu(1)\, 2^6 = 2 - 4 - 8 + 64 = 54.$

Extra Exercises:

6. Suppose that an RSA cryptosystem has public key $(454980781, 17)$. Given that the prime factorization of 454980781 is 15581×29201, find the decryption exponent.

Solution: We have $\phi(454980781) = 15580 \times 29200 = 454936000$, so we need to find the inverse of 17 modulo 454936000. The table produced by the extended Euclidean Algorithm is as follows (we actually don't need the fourth row):

454936000	17	3	2	1	0
		26760941	5	1	2
0	1	26760941^-	133804706	160565647^-	
1	0	1	5^-	6	

The conclusion is that $17 \times (-160565647) \equiv 1 \pmod{454936000}$, and so the required inverse of 17 is $454936000 - 160565647 = 294370353$.

***7.** Let n be a positive integer. Prove that

$$\sum_{d|n} \frac{\mu(d)^2}{\phi(d)} = \frac{n}{\phi(n)},$$

where ϕ is Euler's phi function, μ is the Möbius function, and the sum on the left-hand side is over all positive integer divisors of d.

Solution: Since μ and ϕ are multiplicative functions, the function $\frac{\mu(n)^2}{\phi(n)}$ is also multiplicative. Hence the left-hand side of the desired equation is a multiplicative function of n, by a result from lectures. The right-hand side of the desired equation is also a multiplicative function of n. So it suffices to prove the equality when $n = p^k$, where p is prime and $k \geq 1$.

In this case, the left-hand side becomes

$$\sum_{i=0}^{k} \frac{\mu(p^i)^2}{\phi(p^i)} = \frac{\mu(1)^2}{\phi(1)} + \frac{\mu(p)^2}{\phi(p)} = 1 + \frac{1}{p-1} = \frac{p}{p-1},$$

because $\mu(p^i) = 0$ when $i \geq 2$. The right-hand side becomes

$$\frac{p^k}{p^k - p^{k-1}} = \frac{p}{p-1}.$$

So the equality is true when $n = p^k$ and hence always.

8. (a) For which values of $n \in \mathbb{Z}^+$ is Euler's phi function odd?

Solution: Assume that $\phi(n)$ is odd. Let $n = p_1^{\alpha_1} \cdots p_d^{\alpha_d}$. Then

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_d^{\alpha_d - 1}(p_d - 1)$$

If one of the p_i's is odd then $p_i - 1$ is even and so $\phi(n)$ is. Therefore n must be of the form $n = 2^\alpha$. By computing

$$\phi(2^\alpha) = \begin{cases} 2^{\alpha-1} & \alpha \geq 1 \\ 1 & \alpha = 0 \end{cases}$$

we get that $\phi(n)$ is only odd for $n = 1$ and $n = 2$.

(b) Find all values $n \in \mathbb{Z}^+$ (if any) that solve

$$\phi(n) = \frac{n}{2}.$$

Solution: From the formula $\phi(n) = n \cdot \prod_{i=1}^{d} \left(1 - \frac{1}{p_i}\right)$ we get that the equation $\phi(n) = n/2$ is equivalent to

$$\frac{1}{2} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_d}\right)$$

which in turn can be rewritten to

$$p_1 p_2 \cdots p_d = 2(p_1 - 1)(p_2 - 1) \cdots (p_d - 1).$$

The left hand side is divisible by two, so one of the primes should be divisible by (and hence equal to) two. Without loss of generality assume that $p_1 = 2$. By substituting this into the equation we get

$$p_2 \cdots p_d = (p_2 - 1) \cdots (p_d - 1)$$

If $d \geq 2$, i.e. if the products on both sides are non-empty we definitely have that the right hand side of the equation is strictly less that the left hand side, which leads to the contradiction. Therefore we also have $d = 1$ and the only possible solutions are $n = 2^k$.

Finally we check that any number $n = 2^k$ with $k \in \mathbb{Z}^+$ satisfies the equation.

(c) Find all values $n \in \mathbb{Z}^+$ (if any) such that $\phi(n) = 98$.

Solution: Firstly notice from the part (a), that the only possible value of k such that $\phi(k)$ is odd is $k = 1, 2$. If n can be written as $n = km$ with coprime k, m and $k, m > 2$ then

$$\phi(n) = \phi(km) = \phi(k)\phi(m)$$

and both factors in the product on the right hand side are even. Therefore $4 \mid \phi(n)$ which is not the case for $\phi(n) = 98$. Therefore n is either of the form p^k or $2p^k$ where p is prime.

One can easily check that $p \neq 2$ since in that case $\phi(p^k)$ as well as$\phi(2p^k)$ is a power of 2.

If $k = 1$ then $\phi(p) = \phi(2p) = p - 1$. Since 99 is not prime, this does not give us any solution.

Finally if $k \geq 2$ then p divides $\phi(p^k) = \phi(2p^k) = p^{k-1}(p-1)$, 98 has only one prime divisor - 7, therefore p should be equal to 7. Finally we check that 98 is never of the form $7^{k-1} \cdot 6$ since three divides $7^{k-1} \cdot 6$ but does not divide 98.

We finally conclude that there are no n such that $\phi(n) = 98$.

****9.** Let n be a positive integer. A complex number z is said to be a *primitive nth root of unity* if $z^n = 1$ and there is no smaller positive integer m such that $z^m = 1$. Use the Möbius Inversion Formula to show that the sum of the primitive nth roots of unity is $\mu(n)$. (Hint: if $n > 1$, the sum of all the complex nth roots of unity is zero, because the coefficient of z^{n-1} in the polynomial $z^n - 1$ is zero.)

Solution: Temporarily, let $\nu(n)$ denote the sum of the primitive nth roots of unity. We want to show that in fact $\nu(n) = \mu(n)$.

Now for every complex root of unity, say z, there is a unique d which is the smallest positive number such that $z^d = 1$; we call d the *order* of z, adopting the terminology that we used in lectures in the context of modular arithmetic. By definition, z has order d if and only if z is a primitive dth root of unity. If so, then by the same argument as in the setting of modular arithmetic, every other exponent n for which $z^n = 1$ must be a multiple of the order d; conversely, if n is a multiple of d then certainly $z^n = 1$. Therefore, the set of all complex nth roots of unity (that is, the set $\{\cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) \mid 0 \leq k < n\}$) is the disjoint union of the sets of primitive dth roots of unity as d runs over all positive divisors of n.

Hence $\sum_{d|n} \nu(d)$ equals the sum of all the complex nth roots of unity. This sum is 1 when $n = 1$ (because the only 1st root of unity is 1 itself), and zero when $n > 1$ as noted in the hint. So for all positive integers n we have

$$\sum_{d|n} \nu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases}$$

But by a result in lectures, $\sum_{d|n} \mu(d)$ is given by the same formula. Hence the Möbius Inversion Formula shows that $\nu(n) = \mu(n)$ for all n.