THE UNIVERSITY OF SYDNEY
SCHOOL OF MATHEMATICS AND STATISTICS

Solutions to Tutorial 4 (Week 5)

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. To find the inverse of 5 modulo a prime $p > 5$, it is enough to find integers r, s such that $5r + sp = 1$. Then the inverse of 5 modulo p is r; more correctly, any element of the congruence class of r mod p is **an** inverse of 5 modulo p. Find inverses of 5 modulo the following primes: 7, 11, 13, 17. (Hint: you could use the extended Euclidean Algorithm to find r, s, but for these small values of p, it may be quicker just to look for a small positive integer s such that sp ends in a 1 or a 6.)

Solution: Since $3 \times 7 = 21$ ends in a 1, we have $3 \times 7 \equiv 1 \pmod 5$, and more specifically $3 \times 7 = 1 + 4 \times 5$. This can be rearranged to the form specified in the question: $(-4) \times 5 + 3 \times 7 = 1$. So the inverse of 5 modulo 7 is -4, up to congruence modulo 7; thus, 3 (for instance) is an equally acceptable answer.

Similarly, inverses of 5 modulo 11, 13, 17 are, respectively, -2 (or 9 or ...), -5 (or 8 or ...), -10 (or 7 or ...).

2. Solve the following systems of simultaneous congruences.

(a) $\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 5 \pmod{13} \end{cases}$

Solution: The congruence $x \equiv 2 \pmod 7$ is equivalent to saying that $x = 2 + 7k$ for some $k \in \mathbb{Z}$. Substituting this in the second congruence and subtracting 2 from both sides gives $7k \equiv 3 \pmod{13}$. Since 7 and 13 are coprime, we can get an equivalent congruence by multiplying both sides by the inverse of 7 modulo 13, which is 2 since $2 \times 7 \equiv 1 \pmod{13}$. This gives $k \equiv 6 \pmod{13}$, or in other words $k = 6 + 13l$ for some $l \in \mathbb{Z}$. Thus $x = 2 + 7(6 + 13l) = 44 + 91l$ for some $l \in \mathbb{Z}$, which is equivalent to saying that $x \equiv 44 \pmod{91}$. We have thus found the solution: the original pair of congruences is equivalent to the single congruence $x \equiv 44 \pmod{91}$. So $x = 44$ is one specific integer which satisfies the two original congruences, but so is $x = 44 + 91 = 135$, and so is $x = 44 - 91 = -47$, etc.

(b) $\begin{cases} 2x \equiv 2 \pmod 7 \\ 3x \equiv 6 \pmod{12} \end{cases}$

Solution: We can simplify both of these congruences to remove the coefficients of x. Since 2 and 7 are coprime, 2 has an inverse modulo 7, namely 4; multiplying both sides of $2x \equiv 2 \pmod 7$ by 4, we get that it is equivalent to $x \equiv 1 \pmod 7$. Since 3 divides 12 (and also 6, which is important because $3x \equiv 5 \pmod{12}$, for instance, would have no solutions at all), we get a congruence equivalent to $3x \equiv 6 \pmod{12}$ by dividing **all** numbers by 3: namely, $x \equiv 2 \pmod 4$. So the original system is equivalent to the system

$$\begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 2 \pmod 4 \end{cases}$$

This can be solved in the same way as the previous part: the solution is $x \equiv 22 \pmod{28}$.

(c) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 9 \pmod{11} \end{cases}$

Solution: The first congruence is equivalent to saying that $x = 1 + 3k$ for some $k \in \mathbb{Z}$. Substituting this in the second congruence gives $3k \equiv 1 \pmod 5$, which is equivalent to $k \equiv 2 \pmod 5$; in other words, $k = 2 + 5l$ for some $l \in \mathbb{Z}$. Hence $x = 1 + 3(2 + 5l) = 7 + 15l$ for some $l \in \mathbb{Z}$, and the solution to the system formed by just the first two congruences would be $x \equiv 7 \pmod{15}$. Substituting $x = 7 + 15l$ into the third congruence gives $15l \equiv 2 \pmod{11}$, which can be alternatively written as $4l \equiv 2 \pmod{11}$. Multiplying both sides by 3 which is the inverse of 4 modulo 11, we see that this congruence is equivalent to $l \equiv 6 \pmod{11}$, i.e. $l = 6 + 11m$ for some $m \in \mathbb{Z}$. So $x = 7 + 15(6 + 11m) = 97 + 165m$. The solution is $x \equiv 97 \pmod{165}$.

(d) $\begin{cases} 3x \equiv 1 \pmod 7 \\ 2x \equiv 10 \pmod{16} \\ 5x \equiv 1 \pmod{18} \end{cases}$

Solution: Simplifying the congruences to remove the coefficients of x gives an equivalent system:

$$\begin{cases} x \equiv 5 \pmod 7 \\ x \equiv 5 \pmod 8 \\ x \equiv 11 \pmod{18} \end{cases}$$

The solution to the system consisting of just the first two congruences is clearly $x \equiv 5 \pmod{56}$, i.e. $x = 5 + 56k$ for some $k \in \mathbb{Z}$. Substituting this in the third congruence gives $56k \equiv 6 \pmod{18}$, which is equivalent to $2k \equiv 6 \pmod{18}$ and hence to $k \equiv 3 \pmod 9$. Hence $x = 5 + 56(3 + 9l) = 173 + 504l$ for some $l \in \mathbb{Z}$. So the solution is $x \equiv 173 \pmod{504}$.

3. Find the residues of 2^{2016} modulo the numbers 3, 11, 23, 759 ($= 3 \times 11 \times 23$). (Hint: use Fermat's Little Theorem for the primes 3, 11, 23, and then solve a system of congruences for 759.)

Solution: Fermat's Little Theorem implies that when p is a prime different from 2 we have $2^{p-1} \equiv 1 \pmod p$, and hence $2^n \equiv 2^r \pmod p$ where r is the residue of n modulo $p - 1$. Now

$$2016 \equiv 0 \pmod 2, \text{ so } 2^{2016} \equiv 2^0 \equiv 1 \pmod 3;$$
$$2016 \equiv 6 \pmod{10}, \text{ so } 2^{2016} \equiv 2^6 \equiv 9 \pmod{11};$$
$$2016 \equiv 14 \pmod{22}, \text{ so } 2^{2016} \equiv 2^{14} \equiv 8 \pmod{23}.$$

To find the residue of 2^{2016} modulo 759, it suffices to solve the following system of congruences:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 9 \pmod{11} \\ x \equiv 8 \pmod{23} \end{cases}$$

The same method as in the previous question gives the solution $x \equiv 31 \pmod{759}$. So the residue of 2^{2016} modulo 759 is 31.

You may be wondering why we didn't use the Euler–Fermat Theorem to find the residue of 2^{2016} modulo 759. One can compute, using a result from lectures, that $\phi(759) = (3-1)(11-1)(23-1) = 440$, so the Euler–Fermat Theorem tells us that $2^{440} \equiv 1 \pmod{759}$. Since the residue of 2016 modulo 440 is 256, we can conclude that $2^{2016} \equiv 2^{256} \pmod{759}$, but 2^{256} is still too large for a calculator, so this doesn't immediately solve the problem. However, the next question gives an alternative method of finding residues of powers, and in that method, 2^{256} is easier to work with than 2^{2016} because 256 happens to be a power of 2. So the Euler–Fermat Theorem is indeed useful in this context.

4. This question offers an alternative method for finding residues of powers such as a^{2016}. We use the fact that in binary, the number 2016 is written 11111100000; this indicates how to write 2016 as a sum of powers of 2, namely

$$2016 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 = 1024 + 512 + 256 + 128 + 64 + 32.$$

(a) Note that in the sequence 3^1, 3^2, 3^4, 3^8, 3^{16}, $\ldots$, each term is the square of the one preceding it. By repeatedly squaring and reducing modulo 23, find the residue of 3^{2^k} modulo 23 for $k = 0, 1, 2, \ldots, 10$.

Solution: We have, always working mod 23:

$$\begin{aligned} 3^1 &\equiv 3, \\ 3^2 &\equiv 9, \\ 3^4 &\equiv 81 \equiv 12, \\ 3^8 &\equiv 144 \equiv 6, \\ 3^{16} &\equiv 36 \equiv 13, \\ 3^{32} &\equiv 169 \equiv 8, \\ 3^{64} &\equiv 64 \equiv 18, \\ 3^{128} &\equiv 324 \equiv 2, \\ 3^{256} &\equiv 4, \\ 3^{512} &\equiv 16, \\ 3^{1024} &\equiv 256 \equiv 3. \end{aligned}$$

(The order of 3 modulo 23 is 11, so we could also have calculated these residues by reducing the exponents modulo 11.)

(b) Hence find the residue of 3^{2016} modulo 23.

Solution: We have

$$3^{2016} = 3^{1024+512+256+128+64+32} = 3^{1024}3^{512}3^{256}3^{128}3^{64}3^{32},$$

so we can multiply the relevant residues calculated in the previous part to find that

$$3^{2016} \equiv 3 \times 16 \times 4 \times 2 \times 18 \times 8 \equiv 4 \pmod{23}.$$

***5.** Let p be a prime number.

(a) Show that the binomial coefficient $\binom{p}{i}$ is divisible by p when $1 \leq i \leq p-1$.

Solution: Recall that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. Since p is prime, it does not divide any of the factorials $1!, 2!, \cdots, (p-1)!$. Thus, when $1 \leq i \leq p-1$ we know that p divides $p! = \binom{p}{i} i!\,(p-i)!$ but does not divide either $i!$ or $(p-i)!$, so it must divide $\binom{p}{i}$.

(b) Suppose that $1 \leq m \leq p-1$ and $0 \leq i \leq mp$. Show that the binomial coefficient $\binom{mp}{i}$ is divisible by p if and only if i is not divisible by p.

Solution: As in the previous part, the main idea is to consider the factors of p in the equation

$$(mp)! = \binom{mp}{i} i!\,(mp-i)!.$$

Since $m \leq p-1$, the exponent of p in the prime factorization of $(mp)!$ is m, because p occurs once in the prime factorizations of p, $2p$, $\ldots$, mp and not at all in the prime factorizations of the other positive integers less than or equal to mp. Similarly, the exponent of p in the prime factorization of $i!$ is $\lfloor i/p \rfloor$, the greatest integer less than or equal to i/p, and the exponent of p in the prime factorization of $(mp-i)!$ is $\lfloor (mp-i)/p \rfloor$. So the exponent of p in the prime factorization of $\binom{mp}{i}$ is $m - \lfloor i/p \rfloor - \lfloor (mp-i)/p \rfloor$. Using the rules that $\lfloor x+k \rfloor = \lfloor x \rfloor + k$ when k is an integer and that $-\lfloor -x \rfloor = \lceil x \rceil$ (the smallest integer greater than or equal to x), we can rewrite this exponent as $\lceil i/p \rceil - \lfloor i/p \rfloor$, which is 1 if i/p is not an integer and 0 if i/p is an integer. We conclude that $\binom{mp}{i}$ is divisible by p if and only if i/p is not an integer, as desired.

Extra Exercises:

6. Find the residue of 2^{2016} modulo 385.

Solution: The prime factorization of 385 is $5 \times 7 \times 11$, so we first find the residues of 2^{2016} modulo 5, 7 and 11 as in Q3: they are 1, 1, and 9. We then need to solve the following system of congruences:

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{7} \\ x \equiv 9 \pmod{11} \end{cases}$$

The solution is $x \equiv 141 \pmod{385}$, so the residue of 2^{2016} modulo 385 is 141.

Alternatively we could use the method of Q4, but having to reduce squares mod 385 would be time-consuming. If we know that $\phi(385) = (5-1)(7-1)(11-1) = 240$, then the Euler–Fermat Theorem tells us that $2^{2016} \equiv 2^{96} \pmod{385}$, which makes the calculation a bit shorter.

7. Find, if possible, inverses modulo 84 of the following numbers: $17, 83, 33, 23$.

Solution: Recall that an inverse of a modulo 84 is an integer r such that $ar \equiv 1 \pmod{84}$. Such an inverse exists if and only if $\gcd(a, 84) = 1$; if so, an inverse can be found using the extended Euclidean Algorithm, which in fact finds integers r, s such that $ar + 84s = 1$. But for particular values of a, there may be shorter ways.

When $a = 17$, there is a small value of r which works, namely $r = 5$, since $5 \times 17 = 85 \equiv 1 \pmod{84}$. Note that 5 is not the unique inverse: any integer congruent to 5 modulo 84 would do.

When $a = 83$, we have $a \equiv -1 \pmod{84}$, so -1 is an inverse of 83 modulo 84, as is 83 itself.

When $a = 33$ we have $\gcd(33, 84) = 3 \neq 1$, so 33 has no inverse modulo 84.

When $a = 23$ we probably have to use the extended Euclidean Algorithm:

$$\begin{array}{cccccc c}
84 & 23 & 15 & 8 & 7 & 1 & 0 \\
 & & 3 & 1 & 1 & 1 & 7 \\
0 & 1 & 3^{-} & 4 & 7^{-} & 11 & \\
1 & 0 & 1 & 1^{-} & 2 & 3^{-} &
\end{array}$$

We conclude that $1 = (-3) \times 84 + 11 \times 23$, so an inverse of 23 modulo 84 is 11.

8. Solve the following systems of simultaneous congruences.

(a) $\begin{cases} 4x \equiv 15 \pmod{37} \\ 23x \equiv 5 \pmod{84} \end{cases}$

Solution: An inverse of 4 modulo 37 is -9, and an inverse of 23 modulo 84 is 11, as seen in the previous question. Multiplying the congruences by these inverses, we see that an equivalent system is:

$$\begin{cases} x \equiv 13 \pmod{37} \\ x \equiv 55 \pmod{84} \end{cases}$$

Setting $x = 13 + 37k$ in the second congruence, and simplifying, gives $37k \equiv 42 \pmod{84}$. Since $\gcd(37, 84) = 1$, there is a unique solution of this congruence modulo 84. Since 42 is exactly half of 84, it is clear that $37 \times 42 \equiv 42 \pmod{84}$ just because 37 is odd. So $k \equiv 42 \pmod{84}$ is the unique solution of $37k \equiv 42 \pmod{84}$. Writing this as $k = 42 + 84l$ and substituting in the formula for x, we get $x = 13 + 37(42 + 84l) = 1567 + 3108l$. So the solution is $x \equiv 1567 \pmod{3108}$.

(b) $\begin{cases} 3x \equiv 1 \pmod{5} \\ 2x \equiv 10 \pmod{12} \\ 7x \equiv 2 \pmod{17} \end{cases}$

Solution: Simplifying each congruence individually, we see that an equivalent system is

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 10 \pmod{17} \end{cases}$$

The solution of the system consisting of just the first and second congruences is clearly $x \equiv 17 \pmod{30}$. Substituting $x = 17 + 30k$ into the third congruence, and simplifying, gives $13k \equiv 10 \pmod{17}$. The inverse of 13 modulo 17 is 4, so this is equivalent to $k \equiv 40 \equiv 6 \pmod{17}$. Substituting $k = 6 + 17l$ into the formula for x gives $x = 17 + 30(6 + 17l) = 197 + 510l$. So the solution is $x \equiv 197 \pmod{510}$.

****9.** Define a sequence of integers s_n, $n \in \mathbb{N}$, by

$$s_0 = 2, \quad s_1 = 4, \quad s_n = 4s_{n-1} - s_{n-2} \text{ for all } n \geq 2.$$

(a) Give a closed formula for s_n in terms of the roots of the polynomial $x^2 - 4x + 1$.

Solution: The polynomial $x^2 - 4x + 1$ has roots $2 \pm \sqrt{3}$, so the general solution of the recurrence $s_n = 4s_{n-1} - s_{n-2}$ is $s_n = C(2+\sqrt{3})^n + D(2-\sqrt{3})^n$. In our case the initial conditions $s_0 = 2$ and $s_1 = 4$ give $C = D = 1$, so

$$s_n = (2 + \sqrt{3})^n + (2 - \sqrt{3})^n.$$

(b) Use the binomial theorem to rewrite the formula for s_n so that it involves only integers.

Solution: Applying the binomial theorem, we have

$$\begin{aligned} s_n &= \left(\sum_{i=0}^{n} \binom{n}{i} 2^{n-i} (\sqrt{3})^i \right) + \left(\sum_{i=0}^{n} \binom{n}{i} 2^{n-i} (-\sqrt{3})^i \right) \\ &= \sum_{i=0}^{n} \binom{n}{i} 2^{n-i} ((\sqrt{3})^i + (-\sqrt{3})^i) \\ &= \sum_{\substack{i=0 \\ i \text{ even}}}^{n} \binom{n}{i} 2^{n-i+1} (\sqrt{3})^i \\ &= \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} 2^{n-2j+1} 3^j. \end{aligned}$$

Here the third equality used the fact that $(\sqrt{3})^i + (-\sqrt{3})^i = 0$ if i is odd, and the fourth equality used the substitution $i = 2j$. As usual, $\lfloor n/2 \rfloor$ denotes the largest integer less than or equal to $n/2$.

(c) Show that if p is a prime number, then $s_p \equiv 4 \pmod{p}$.

Solution: If $n = p$ is a prime number, Q5 tells us that all the binomial coefficients appearing in the formula for s_p will be divisible by p except for $\binom{p}{0} = 1$ in the $j = 0$ term and $\binom{p}{p} = 1$ in the $j = p/2$ term, which only exists when $p = 2$. So if $p \neq 2$ we deduce that $s_p \equiv 2^{p+1} 3^0 \equiv 4 \pmod{p}$, the latter congruence coming from Fermat's Little Theorem. If $p = 2$ we have $s_2 = 14 \equiv 4 \pmod{2}$, so the desired congruence holds in either case.