The University of Sydney
School of Mathematics and Statistics

Solutions to Tutorial 10 (Week 12)

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. Solve the congruences $x^2 \equiv 2 \pmod{17}$, $x^2 \equiv 2 \pmod{19}$ and $x^2 \equiv 2 \pmod{23}$.

Solution: We firstly check, which of the equations have solutions. We have $2^8 \equiv 1 \pmod{17}$ and $2^{11} \equiv 1 \pmod{23}$ whereas $2^9 \equiv -1 \pmod{23}$. So the congruences $x^2 \equiv 2 \pmod{17}$ and $x^2 \equiv 2 \pmod{23}$ have solutions, whereas the other one $x^2 \equiv 2 \pmod{19}$ does not.

Since $23 \equiv 3 \pmod 4$, square roots modulo 23 are easy to find: in general, if a is a quadratic residue modulo 23, then $a^{(23+1)/4} = a^6$ is a square root of a modulo 23. We deduce that $2^6 \equiv -5$ is a square root of 2 modulo 23; alternatively, we might just have noticed that $2 \equiv 25 \pmod{23}$. So the solutions of $x^2 \equiv 2 \pmod{23}$ are $x \equiv \pm 5 \pmod{23}$.

Since $17 \equiv 1 \pmod 4$, the general rule for finding square roots modulo 17 involves more work than finding square roots modulo 23, and for a small prime like 17 it is quicker just to go through all the possibilities. We find that the solutions of $x^2 \equiv 2 \pmod{17}$ are $x \equiv \pm 6 \pmod{17}$.

2. Given that $1081 = 23 \times 47$, solve the congruence $x^2 \equiv 2 \pmod{1081}$.

Solution: An integer x is a solution of $x^2 \equiv 2 \pmod{1081}$ if and only if it is simultaneously a solution of $x^2 \equiv 2 \pmod{23}$ and a solution of $x^2 \equiv 2 \pmod{47}$. (Here the "if" direction uses the Chinese Remainder Theorem.) As seen in Q1, the solutions of $x^2 \equiv 2 \pmod{23}$ are $x \equiv \pm 5 \pmod{23}$. By the same method, we find that the solutions of $x^2 \equiv 2 \pmod{47}$ are $x \equiv \pm 7 \pmod{47}$. So there are four congruence classes modulo 1081 that are solutions of $x^2 \equiv 2$, obtained by making all possible choices of signs in the simultaneous congruences $x \equiv \pm 5 \pmod{23}$ and $x \equiv \pm 7 \pmod{47}$.

We first solve $x \equiv 5 \pmod{23}$ and $x \equiv 7 \pmod{47}$ simultaneously. Substituting $x = 5 + 23k$ into the second congruence gives $23k \equiv 2 \pmod{47}$. Since -2 is an inverse of 23 modulo 47, this is equivalent to $k \equiv -4 \pmod{47}$. Hence we get $x \equiv 5 - 23 \times 4 = -87 \pmod{1081}$.

We now solve $x \equiv 5 \pmod{23}$ and $x \equiv -7 \pmod{47}$ simultaneously. Substituting $x = 5 + 23k$ into the second congruence gives $23k \equiv -12 \pmod{47}$, which is equivalent to $k \equiv 24 \pmod{47}$. Hence we get $x \equiv 5 + 23 \times 24 = 557 \pmod{1081}$.

There is no need to go through the other two cases, since they must result in the negatives of the two solutions we have already found. So the solutions of $x^2 \equiv 2 \pmod{1081}$ are $x \equiv \pm 87 \pmod{1081}$ and $x \equiv \pm 557 \pmod{1081}$.

3. Bob, a user of Rabin's cryptosystem, posts the public key 826277. Alice sends Bob the single-letter ciphertext 43792. Use Fermat's factorization method to find the prime factors of 826277, and hence find the four possibilities for Alice's message before encryption.

Solution: Since $\lceil\sqrt{826277}\rceil = 909$, we calculate $909^2 - 826277$ and find that it equals 4. Hence

$$826277 = 909^2 - 2^2 = 907 \times 911.$$

Assuming that Bob has followed the correct procedures for this cryptosystem, his public key must be the product of two primes, so we can conclude that 907 and 911 are prime (this is fairly quick to check by trial division). Now we need to solve $x^2 \equiv 43792 \pmod{826277}$. Since 43792 has residue 256 modulo 907 and residue 64 modulo 911, this is equivalent to solving $x^2 \equiv 256 \pmod{907}$ and $x^2 \equiv 64 \pmod{911}$ simultaneously. Since these residues happen to be perfect squares, the solutions are obvious: $x^2 \equiv 256 \pmod{907}$ has solutions $x \equiv \pm 16 \pmod{907}$, and $x^2 \equiv 64 \pmod{911}$ has solutions $x \equiv \pm 8 \pmod{911}$.

Solving $x \equiv 16 \pmod{907}$ and $x \equiv 8 \pmod{911}$ simultaneously gives $x \equiv 1830 \pmod{826277}$. Solving $x \equiv 16 \pmod{907}$ and $x \equiv -8 \pmod{911}$ simultanously gives $x \equiv 5458 \pmod{826277}$. The other solutions must then be $x \equiv -1830 \equiv 824447 \pmod{826277}$ and $x \equiv -5458 \equiv 820819 \pmod{826277}$. So the four possibilities for Alice's single-letter original message are 1830, 5458, 824447 and 820819. Presumably the encoding procedure that Bob has specified enables him to decide which of these is correct.

4. Let p be an odd prime and d an odd divisor of $p-1$. As seen in lectures, the set $X = \{a \in \{1, \cdots, p-1\} \mid a^d \equiv 1 \pmod{p}\}$ has exactly d elements. Show that the function $f : X \to X$ defined by letting $f(x)$ be the residue of x^2 modulo p is invertible.

Solution: First note that f is well defined, because if $x \in X$ then $f(x)^d \equiv (x^2)^d \equiv (x^d)^2 \equiv 1^2 \equiv 1 \pmod{p}$. Now define another function $g : X \to X$ by letting $g(x)$ be the residue of $x^{(d+1)/2}$ modulo p; this is well defined for a similar reason. For any $x \in X$, we have

$$f(g(x)) \equiv g(x)^2 \equiv (x^{(d+1)/2})^2 \equiv x^{d+1} \equiv x \pmod{p},$$

where the last congruence is because $x^d \equiv 1 \pmod{p}$ by definition of X. An entirely similar calculation shows that $g(f(x)) = x$, so the functions f and g are inverse to each other.

5. The aim of this question is to solve the congruence $x^2 \equiv 20 \pmod{41}$, following the procedure given in lectures for finding square roots modulo a prime congruent to 1 modulo 4.

(a) The first step is to check that 20 is a quadratic residue modulo 41. Do this by repeatedly squaring and reducing modulo 41 to find the residues of 20^2, 20^4, 20^8 and 20^{16} modulo 41, then conclude that $20^{20} \equiv 1 \pmod{41}$ as required.

Solution: We have $20^2 \equiv 31$, $20^4 \equiv 18$, $20^8 \equiv 37$ and $20^{16} \equiv 16 \pmod{41}$. Hence $20^{20} \equiv 16 \times 18 \equiv 1 \pmod{41}$, showing that 20 is a quadratic residue modulo 41.

(b) The next step is to find an element b of $\{1, 2, \cdots, 40\}$ which has order 8 modulo 41 (where 8 is relevant because it is the highest power of 2 dividing 40). For this, use the information that $3^{20} \equiv -1 \pmod{41}$.

Solution: The fact that $3^{20} \equiv -1 \pmod{41}$ means that 3^5 has order 8 modulo 41, as seen in lectures. So we can take b to be the residue of 3^5 modulo 41, which is 38 (actually, -3 would do just as well).

(c) We then must have $b^{2j} \equiv 20^5 \pmod{41}$ for some $j \in \{0, 1, 2, 3\}$. Find j.

Solution: We have $20^5 \equiv 18 \times 20 \equiv 32 \pmod{41}$, so the congruence we are trying to solve is $9^j \equiv 32 \pmod{41}$. It is easy to see that $j = 3$ works.

(d) Finally, use this information to solve $x^2 \equiv 20 \pmod{41}$.

Solution: We have that $38^6 \equiv 20^5 \pmod{41}$. If we multiply both sides of this congruence by 20^{-4} (meaning an inverse modulo 41 of 20^4), then we get $20 \equiv (38^3 \times 20^{-2})^2 \pmod{41}$, so $x = 38^3 \times 20^{-2}$ is a solution of $x^2 \equiv 20 \pmod{41}$. Now an inverse of 20 is -2, so we can replace 20^{-2} by 4; also, we can replace 38^3 by $(-3)^3 \equiv -27 \equiv 14$. So $x = 56 \equiv 15$ is a solution of $x^2 \equiv 20 \pmod{41}$, and the complete solution must be $x \equiv \pm 15 \pmod{41}$.

6. Let p be an odd prime, $k \geq 2$ an integer, and a an integer such that $\gcd(a, p) = 1$. This question concerns the solutions of the congruence $x^2 \equiv a \pmod{p^k}$.

(a) Take $p = 3$ and $a = 7$. Solve $x^2 \equiv 7 \pmod{3^k}$ for $k = 2, 3, 4$.

Solution: The solutions of $x^2 \equiv 7 \pmod{9}$ are easily seen to be $x \equiv \pm 4 \pmod{9}$. Therefore, when we try to solve $x^2 \equiv 7 \pmod{27}$, we need only test those residues mod 27 which are congruent to ± 4 modulo 9; then it is easy to find that the solutions are $x \equiv \pm 13 \pmod{27}$. Therefore, when we try to solve $x^2 \equiv 7 \pmod{81}$, we need only test those residues mod 81 which are congruent to ± 13 modulo 27; then it is easy to find that the solutions are $x \equiv \pm 13 \pmod{81}$. Notice that we found exactly two solutions in each case, which illustrates the next two parts of the question.

*(b) Show that $x^2 \equiv a \pmod{p^k}$ either has no solutions or has exactly two solutions up to congruence mod p^k.

Solution: If x is a solution then clearly $-x$ is also a solution, and $-x \not\equiv x \pmod{p^k}$. So we just need to show that there cannot be more than two solutions. Suppose for a contradiction that $x^2 \equiv y^2 \equiv a \pmod{p^k}$ with $y \not\equiv \pm x \pmod{p^k}$. Then p^k divides $x^2 - y^2 = (x - y)(x + y)$ but does not divide either $x - y$ or $x + y$. We can conclude that the factors of p are split in some way between $x - y$ and $x + y$; in particular, p divides both $x - y$ and $x + y$, implying that p divides $2x$. But p is an odd prime, so this forces p to divide x and hence a, which contradicts the assumption that $\gcd(a, p) = 1$.

An alternative approach is to use the fact (proved in Q5 of Tutorial 8) that there exists a primitive root b modulo p^k. Since $\gcd(a, p) = 1$, we have $a \equiv b^i \pmod{p^k}$ for some $i \in \{0, 1, \cdots, \phi(p^k) - 1\}$. Any solution x of $x^2 \equiv a \pmod{p^k}$ would also have to satisfy $\gcd(x, p) = 1$, and we would hence have $x \equiv b^j \pmod{p^k}$ for some $j \in \{0, 1, \cdots, \phi(p^k) - 1\}$, making the congruence $x^2 \equiv a \pmod{p^k}$ equivalent to $b^{2j} \equiv b^i \pmod{p^k}$, which in turn is equivalent to $2j \equiv i \pmod{\phi(p^k)}$. Since $\phi(p^k) = p^{k-1}(p - 1)$ is even, the latter congruence forces i to be even, and then the two solutions are given by $j = i/2$ and $j = (i + \phi(p^k))/2$.

**(c) Show that $x^2 \equiv a \pmod{p^k}$ has solutions if and only if $x^2 \equiv a \pmod{p}$ has solutions.

Solution: The "only if" direction is easy: the congruence $x^2 \equiv a \pmod{p^k}$ implies the congruence $x^2 \equiv a \pmod{p}$ by basic principles of congruences. So we need only prove the "if" direction.

One approach is to consider all the congruences $x^2 \equiv a \pmod{p^k}$ together as a varies. Let A denote the standard reduced system modulo p^k, consisting of those elements $a \in \{1, \cdots, p^k - 1\}$ such that $\gcd(a, p) = 1$; then $|A| = \phi(p^k) = p^{k-1}(p - 1)$. We can define a function $f : A \to A$ by setting $f(x)$ to be the residue of x^2 modulo p^k. The result of the previous part means that f is a 2-to-1 function, so the range of f has size $|A|/2$. But if a belongs to the range of f, then $x^2 \equiv a \pmod{p^k}$ has a solution, so by the "only if" direction already seen, the residue of a modulo p is a quadratic residue. Let B be the subset of A consisting of elements a such that the residue of a modulo p is a quadratic residue. Since exactly half of the nonzero residues mod p are quadratic residues, and the residues mod p of the elements of A are evenly distributed over the nonzero residues, $|B| = |A|/2$. We conclude that B equals the range of f, which is what we needed to show.

Again, an alternative approach is to use the fact that there exists a primitive root b modulo p^k, which is then necessarily also a primitive root modulo p. We have $a \equiv b^i \pmod{p^k}$ for some $i \in \{0, 1, \cdots, \phi(p^k) - 1\}$, and hence $a \equiv b^r \pmod{p}$ where r is the residue of i modulo $\phi(p) = p - 1$. Since $x^2 \equiv a \pmod{p}$ has solutions, r is even, which implies that i is even, so $x^2 \equiv a \pmod{p^k}$ has solutions.

Extra Exercises:

7. Given that $29647 = pq$ for distinct primes p and q, and that 2577 is a square root of 1 modulo 29647, find p and q.

Solution: The fact that 2577 is a square root of 1 modulo 29647 tells us that $29647 = pq$ divides $2577^2 - 1 = 2576 \times 2578$. So one of the two primes, say p, must divide 2576 and the other, say q, must divide 2578. Hence $p = \gcd(29647, 2576)$ and $q = \gcd(29647, 2578)$, and we can find them using the Euclidean Algorithm. For instance,

$$29647 = 11 \times 2578 + 1289$$
$$2578 = 2 \times 1289 + 0$$

This shows that $q = 1289$, so $p = 23$.

This exercise illustrates that if one can solve the square root problem modulo m (where m is the product of two unknown primes), then one can factorize m. Conversely, as seen in lectures, if one can factorize m, one can solve the square root problem modulo m.

8. Suppose that p is a prime such that $p \equiv 7 \pmod 9$, and a is an integer such that $\gcd(a,p) = 1$. Show that if the congruence $x^3 \equiv a \pmod p$ has solutions, then $x = a^{(p+2)/9}$ is one solution.

Solution: We are assuming that there is some integer x such that $x^3 \equiv a \pmod p$. Since $a \not\equiv 0 \pmod p$, we must also have $x \not\equiv 0 \pmod p$. So $x^{p-1} \equiv 1$ by Fermat's Little Theorem. Since $p \equiv 1 \pmod 3$, we can conclude that $a^{(p-1)/3} \equiv (x^3)^{(p-1)/3} \equiv x^{p-1} \equiv 1 \pmod p$. Hence

$$(a^{(p+2)/9})^3 = a^{(p+2)/3} = a^{(p-1)/3}a \equiv a \pmod p,$$

as required.

9. Use the facts that $3^{36} \equiv 1 \pmod{73}$ and $\mathrm{ord}_{73}(10) = 8$ to solve $x^2 \equiv 3 \pmod{73}$.

Solution: Note that 73 is a prime congruent to 1 modulo 4. In fact, $73 - 1 = 72$ has prime factorization $2^3 \times 3^2$, which is why it is important for this calculation to know an element which has order $8 = 2^3$ modulo 73. Specifically, as seen in lectures, the fact that $\mathrm{ord}_{73}(10) = 8$ means that the four 4th roots of 1 modulo 73 are $10^0 \equiv 1$, $10^2 \equiv 27$, $10^4 \equiv -1 \equiv 72$ and $10^6 \equiv -27 \equiv 46$. So we know that 3^9 must be congruent to one of these, and it is easy to check that indeed $3^9 \equiv 46 \equiv 10^6 \pmod{73}$. From this we conclude that the solutions of $x^2 \equiv 3 \pmod{73}$ are $x \equiv \pm 10^3 \times 3^{-4} \pmod{73}$, where 3^{-4} indicates an inverse of $3^4 \equiv 8$, for instance -9. Hence the solutions are $x \equiv \pm 9000 \equiv \pm 21 \pmod{73}$.

***10.** In this exercise we work modulo the prime 941. Note that $(941-1)/4 = 235$.

(a) Use the following table of selected powers of 6 (reduced mod 941) to solve $x^2 \equiv 6 \pmod{941}$.

i	2	4	8	16	32	64	72	73	146	219	235
6^i	36	355	872	56	313	105	283	757	921	857	1

Solution: From the table we see that $6^{470} = (6^{235})^2 \equiv 1 \pmod{941}$. Hence 6 is a quadratic residue mod 941, meaning that $x^2 \equiv 6 \pmod{941}$ has solutions. Better still, the table tells us that $6^{236} \equiv 6$, so the square roots of 6 must be $\pm 6^{118}$. Now 118 in binary is $(1110110)_2$, i.e. $118 = 64+32+16+4+2$, so from the table we see that $6^{118} \equiv 105 \times 313 \times 56 \times 355 \times 36 \equiv 299 \pmod{941}$. So the solutions of $x^2 \equiv 6 \pmod{941}$ are $x \equiv \pm 299 \pmod{941}$, where -299 can be alternatively written as 642.

(b) Use the following table of selected powers of 3 (reduced mod 941) to solve $x^2 \equiv -1 \pmod{941}$.

i	2	4	8	16	32	64	72	73	146	219	235
3^i	9	81	915	676	591	170	285	855	809	60	97

Solution: From the table we see that $3^{235} \not\equiv \pm 1 \pmod{941}$, so $3^{470} = (3^{235})^2 \not\equiv 1 \pmod{941}$. Therefore we must have $3^{470} \equiv -1 \pmod{941}$, meaning that 3 is not a quadratic residue mod 941. This tells us that $97^2 \equiv -1 \pmod{941}$, so the solutions of $x^2 \equiv -1 \pmod{941}$ are $x \equiv \pm 97 \pmod{941}$, where -97 can be alternatively written as 844.

(c) Given that $228^{235} \equiv -1 \pmod{941}$ and that $228^{117} \equiv 267 \pmod{941}$, solve $x^2 \equiv 228 \pmod{941}$. (Hint: consider $(267x)^2$.)

Solution: The first given congruence implies that $228^{470} \equiv 1 \pmod{941}$, so 228 is indeed a quadatic residue mod 941. Suppose that x is a solution of $x^2 \equiv 228 \pmod{941}$. Then $(267x)^2 = 267^2x^2 \equiv 228^{234+1} \equiv -1 \pmod{941}$, so $267x \equiv \pm 97 \pmod{941}$ by the previous part. Now we can use the extended Euclidean algorithm to find an inverse of 267 modulo 941:

941	267	140	127	13	10	3	1	0
		3	1	1	9	1	3	3
0	1	3^-	4	7^-	67	74^-	289	
1	0	1	1^-	2	19^-	21	82^-	

This tells us that 289 is an inverse of 267 modulo 941, so our desired solutions are $x \equiv \pm 289 \times 97 \equiv \mp 197 \pmod{941}$, where -197 can be alternatively written as 744.