The University of Sydney
School of Mathematics and Statistics

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

More difficult questions are marked with either * or **. Those marked * are at the level which MATH2068 students will have to solve in order to be sure of getting a Credit, or to have a chance of a Distinction or High Distinction. Those marked ** are mainly intended for MATH2988 students.

Tutorial Exercises:

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

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

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.

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.

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.

(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 $3^{20} \equiv -1 \pmod{41}$.

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

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

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 $k = 2, 3, 4$.

*(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.

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

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.

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

***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

(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

(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 $(267x)^2$.)

Selected numerical answers:

1. $x \equiv \pm 6 \pmod{17}$, $x \equiv \pm 5 \pmod{23}$ **2.** $x \equiv \pm 87, \pm 557 \pmod{1081}$