The University of Sydney
School of Mathematics and Statistics

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

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. 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.)

2. Solve the following systems of simultaneous congruences.

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

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

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

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

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.)

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}, …, 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 $k = 0, 1, 2, \ldots, 10$.

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

Copyright © 2017 The University of Sydney

*5. Let p be a prime number.

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

(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.

Extra Exercises:

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

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

8. Solve the following systems of simultaneous congruences.

(a) $\begin{cases} 4x \equiv 15 \pmod{37} \\ 23x \equiv 5 \pmod{84} \end{cases}$ (b) $\begin{cases} 3x \equiv 1 \pmod{5} \\ 2x \equiv 10 \pmod{12} \\ 7x \equiv 2 \pmod{17} \end{cases}$

**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.

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

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

Selected numerical answers:
1. 3, 9, 8, 7. **2.** 44 (mod 91), 22 (mod 28), 97 (mod 165), 173 (mod 504).
3. 1, 9, 8, 31.