The University of Sydney
School of Mathematics and Statistics

Tutorial 9 (Week 11)

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. Find a quadratic polynomial $P(x) = ax^2 + bx + c$, where the coefficients a, b, c belong to $\{0, 1, 2, 3, 4, 5, 6\}$, such that the following all hold:

$$\begin{aligned} P(2) &\equiv 5 \pmod 7, \\ P(3) &\equiv 4 \pmod 7, \\ P(5) &\equiv 1 \pmod 7. \end{aligned}$$

2. Given that 7 is a primitive root modulo 71 (which is prime), find the discrete logarithm $\log_{7,71}(3)$, i.e. the unique $x \in \{0, 1, \cdots, 69\}$ such that $7^x \equiv 3 \pmod{71}$. It is quickest to use the Pohlig–Hellman algorithm, i.e. to find the residues of x modulo the prime factors 2, 5, 7 of 70 and then solve the resulting system of congruences for x. You will need the following congruences mod 71:

$$\begin{aligned} 3^{35} &\equiv 1, & 7^{35} &\equiv 70, \\ 3^{14} &\equiv 54, & 7^{14} &\equiv 54, \\ 3^{10} &\equiv 48, & 7^{10} &\equiv 45. \end{aligned}$$

3. 101 is prime, and 2 is a primitive root modulo 101; thus any integer coprime to 101 is congruent modulo 101 to 2^i for some $i \in \{0, 1, \cdots, 99\}$. Find all solutions x of the following congruences which belong to the standard reduced system $\{1, 2, \cdots, 100\}$.

(a) $x^5 \equiv 1 \pmod{101}$

(b) $x^5 \equiv 32 \pmod{101}$

(c) $x^2 \equiv -1 \pmod{101}$

(d) $x^{67} \equiv 10 \pmod{101}$

(e) $x^6 \equiv 4 \pmod{101}$

(f) $x^2 \equiv 2 \pmod{101}$

*__4.__ From the point of view of the Discrete Logarithm Problem, the easiest moduli m to handle are those where $\phi(m)$ has only small prime factors.

(a) For which positive integers m is $\phi(m)$ a power of 2?

(b) For which positive integers m is $\phi(m)$ a power of 3?

(c) For which positive integers m is $\phi(m)$ twice a power of 3?

5. Suppose that for security you want to split the knowledge of a secret positive integer c between four people, P_1, P_2, P_3 and P_4. You choose a prime p larger than c and random positive integers a and b less than p, and tell person P_i the prime p and the number r_i which is the residue of $ai^2 + bi + c$ modulo p. Suppose that each of the four people knows the procedure that you followed, without knowing a, b, c.

(a) How many people need to combine their information to be able to determine c, and how would they do it?

**(b) To what extent would it be less secure to tell each person P_i the actual value n_i of $ai^2 + bi + c$, rather than its residue r_i modulo a chosen prime p?

Extra Exercises:

6. Find $a, b, c \in \{0, 1, \ldots, 18\}$ such that the polynomial $f(x) = ax^2 + bx + c$ satisfies $f(3) \equiv 11$, $f(7) \equiv 2$ and $f(16) \equiv 9 \pmod{19}$.

7. Given that 3 is a primitive root modulo 31, use the Pohlig–Hellman algorithm to find the discrete logarithm $\log_{3,31}(10)$, i.e. the unique $x \in \{0, 1, \cdots, 29\}$ such that $3^x \equiv 10 \pmod{31}$.

8. Given that 5 is a primitive root modulo 257 (which is prime), find the discrete logarithm $\log_{5,257}(2)$, i.e. the unique $x \in \{0, 1, \cdots, 255\}$ satisfying $5^x \equiv 2 \pmod{257}$. (Hint: use the fact that $2^8 \equiv -1 \pmod{257}$ to cut down the possibilities for x.)

***9.** Given that 2 is a primitive root modulo 81 (that is, $\mathrm{ord}_{81}(2) = \phi(81) = 54$), find $\log_{2,81}(5)$, i.e. the unique $x \in \{0, 1, \cdots, 53\}$ satisfying $2^x \equiv 5 \pmod{81}$. (Hint: an efficient method is to solve the congruence $2^x \equiv 5$ modulo 3, then modulo 9, then modulo 27, then modulo 81.)

Selected numerical answers:
1 $x^2 + x + 6$ **2** 26 **3**(a) 1, 36, 84, 87, 95 (b) 2, 67, 72, 73, 89 (c) 10, 91 (d) 91 (e) 26, 75