The University of Sydney
School of Mathematics and Statistics

Tutorial 2 (Week 3)

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. In last week's tutorial, we found $\gcd(a, b)$ in each of the following cases using the Euclidean Algorithm. An alternative method is to use prime factorizations: if a prime p occurs in the prime factorizations of a and b with the exponents k and ℓ respectively (where k and ℓ are allowed to be zero), then p occurs in the prime factorization of $\gcd(a, b)$ with the exponent $\min\{k, \ell\}$. Find the prime factorizations of a and b in each case, and use these to compute $\gcd(a, b)$.

(a) $a = 35$, $b = 14$. (b) $a = 168$, $b = 132$. (c) $a = 847$, $b = 510$.

2. If we have a congruence $k \equiv \ell \pmod{m}$ then we can certainly square both sides to deduce the congruence $k^2 \equiv \ell^2 \pmod{m}$; this is a special case of the validity of multiplying congruences, proved in lectures. The purpose of this exercise is to point out that in general there is no way of going in the other direction, i.e. taking square roots of both sides of a congruence modulo m.

(a) Firstly, not every congruence class modulo m has a square root. To illustrate this, show that there is no integer k such that $k^2 \equiv 2 \pmod{5}$.

(b) Secondly, if k and ℓ are two integers, the congruence $k^2 \equiv \ell^2 \pmod{m}$ does not imply that $k \equiv \pm\ell \pmod{m}$. To illustrate this, find a counterexample with $m = 8$.

(c) On the other hand, show that if p is prime, then $k^2 \equiv \ell^2 \pmod{p}$ does imply that $k \equiv \pm\ell \pmod{p}$.

3. For each $n \in \mathbb{N}$, let a_n be the residue of 2^n modulo 13. Since $a_{k+1} \equiv 2a_k \pmod{13}$ for each $k \in \mathbb{N}$, the a_k are easy to compute recursively, starting with $a_0 = 1$ and then doubling and reducing mod 13 to get successive terms of the sequence. Compute the first dozen or so terms, and then use the pattern you observe to compute a_{2016}.

4. Recall that, if m is a positive integer and a is an integer such that $\gcd(a, m) = 1$, the *order* of a modulo m, written $\mathrm{ord}_m(a)$, is the smallest positive integer j such that $a^j \equiv 1 \pmod{m}$. Find $\mathrm{ord}_m(2)$ for each $m \in \{3, 5, 7, 9, 11, 31\}$.

*5. A *Mersenne prime* is a prime number of the form $2^p - 1$ where p is prime. In fact the words "where p is prime" are redundant in this definition: in order for a number of the form $2^a - 1$ to be prime, a is forced to be prime, by an exercise in last week's tutorial. However, it is not true for all primes p that $2^p - 1$ is prime.

(a) Find the smallest prime p such that $2^p - 1$ is composite.

(b) Suppose that p is prime and q is a prime factor of $2^p - 1$. By considering $\mathrm{ord}_q(2)$ and using Fermat's Little Theorem, show that $q \equiv 1 \pmod{p}$.

Extra Exercises:

6. For many small values of $n \in \mathbb{N}$, the number $n^2 + n + 41$ is prime. For example,

$$0^2 + 0 + 41 = 41,\ 1^2 + 1 + 41 = 43,\ 2^2 + 2 + 41 = 47,\ 3^2 + 3 + 41 = 53$$

are all prime, and this trend continues for a long time. Show that it can't continue forever by specifying a value of n for which $n^2 + n + 41$ is clearly composite.

7. (a) Show that 2, 4, 6, ..., $2m$ constitutes a complete set of residues modulo m, provided m is *odd*.

(b) Show that 1^2, 2^2, 3^2, ..., m^2 is *not* a complete set of residues modulo m, if $m > 2$.

8. Find $\mathrm{ord}_{89}(2)$, $\mathrm{ord}_{17}(3)$ and $\mathrm{ord}_{37}(10)$.

*9. (a) Recall that if m is an odd positive number then we have a factorization identity

$$x^m + 1 = (x + 1)(x^{m-1} - x^{m-2} + \cdots - x + 1).$$

Use this to show that if $2^a + 1$ is prime for $a \in \mathbb{Z}^+$, then $a = 2^k$ for some $k \in \mathbb{N}$.

(b) A prime number of the form $2^{2^k} + 1$ is called a *Fermat prime*: for example,

$$2^1 + 1 = 3,\ 2^2 + 1 = 5,\ 2^4 + 1 = 17,\ 2^8 + 1 = 257,\ 2^{16} + 1 = 65537$$

are all prime. However, show that $2^{32} + 1$ is divisible by 641 using the following observation:

$$641 = 5 \times 2^7 + 1 = 5^4 + 2^4.$$

**10. (For students familiar with analysis.) Assume the following series summation:

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \cdots = \frac{\pi^2}{6}.$$

Deduce that $\dfrac{6}{\pi^2}$ is the limit, as the integer N tends to ∞, of the probability that two independently randomly chosen positive integers a and b less than or equal to N are coprime to each other.

Selected numerical answers:

1. $\gcd(a, b) = 7,\ 12,\ 1$. **3.** $a_{2016} = 1$. **4.** 2, 4, 3, 6, 10, 5.