The University of Sydney
School of Mathematics and Statistics

Solutions to 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

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) $a = 35$, $b = 14$.

Solution: The prime factorizations are $35 = 5 \times 7$ and $14 = 2 \times 7$, so $\gcd(35, 14) = 7$.

(b) $a = 168$, $b = 132$.

Solution: The prime factorizations are $168 = 2^3 \times 3 \times 7$ and $132 = 2^2 \times 3 \times 11$, so $\gcd(168, 132) = 2^2 \times 3 = 12$.

(c) $a = 847$, $b = 510$.

Solution: The prime factorizations are $847 = 7 \times 11^2$ and $510 = 2 \times 3 \times 5 \times 17$, so $\gcd(847, 510) = 1$.

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 $k^2 \equiv 2 \pmod{5}$.

Solution: Every integer k is congruent to either 0, 1, 2, 3 or 4 (mod 5). So k^2 is congruent mod 5 to one of

$$0^2 = 0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 = 9 \equiv 4,\ 4^2 = 16 \equiv 1,$$

i.e. we have either $k^2 \equiv 0$, $k^2 \equiv 1$ or $k^2 \equiv 4 \pmod{5}$. Notice that we didn't really need to work out the residues of 3^2 and 4^2, because $3 \equiv -2 \pmod{5}$ implies that $3^2 \equiv (-2)^2 = 2^2$, and similarly $4^2 \equiv 1^2$.

(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 $m = 8$.

Solution: We compute the residues of the first few squares mod 8:

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 1,\ 4^2 \equiv 0,$$

and there is no need to go further, because $(8-k)^2 \equiv (-k)^2 = k^2 \pmod 8$. So we have multiple counterexamples: for instance, we could take $k = 0$ and $\ell = 4$, or $k = 1$ and $\ell = 3$. Notice that the above calculations show that for any odd integer k we have $k^2 \equiv 1 \pmod 8$.

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

Solution: The meaning of $k^2 \equiv \ell^2 \pmod p$ is that p divides

$$k^2 - \ell^2 = (k-\ell)(k+\ell).$$

As seen in the proof of the Fundamental Theorem of Arithmetic, if a prime divides the product of two integers then it must divide at least one of the two. So $p \mid (k-\ell)(k+\ell)$ implies that either $p \mid k-\ell$ or $p \mid k+\ell$, i.e. either $k \equiv \ell \pmod p$ or $k \equiv -\ell \pmod p$.

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}.

Solution: The sequence a_n begins 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1 – and then it repeats. In other words, $a_0 = a_{12} = a_{24} = \cdots$, and $a_1 = a_{13} = a_{25} = \cdots$, etc. In general, $a_i = a_j$ if and only if $i \equiv j \pmod{12}$. In the terminology introduced in lectures, $\mathrm{ord}_{13}(2) = 12$. Now $2016 \equiv 0 \pmod{12}$; so $a_{2016} = a_0 = 1$.

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 $m \in \{3, 5, 7, 9, 11, 31\}$.

Solution: For each m, we calculate the sequence of residues of $2^n \pmod m$ for $n \in \mathbb{N}$ as in the previous question, until we find the first repetition of 1.

For $m = 3$, the sequence is just 1, 2, 1 (and then it repeats). So $\mathrm{ord}_3(2) = 2$.

For $m = 5$, we get 1, 2, 4, 3, 1, ... So $\mathrm{ord}_5(2) = 4$.

For $m = 7$, we get 1, 2, 4, 1, ... So $\mathrm{ord}_7(2) = 3$.

For $m = 9$, we get 1, 2, 4, 8, 7, 5, 1. So $\mathrm{ord}_9(2) = 6$.

For $m = 11$, we get 1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, ... So $\mathrm{ord}_{11}(2) = 10$.

For $m = 31$, we get 1, 2, 4, 8, 16, 1, ... So $\mathrm{ord}_{31}(2) = 5$.

We can observe that in all these cases, $\mathrm{ord}_m(2)$ is a divisor of $\phi(m)$, in accordance with the Euler–Fermat Theorem.

*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.

Solution: The first four primes p do give Mersenne primes: $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ and $2^7 - 1 = 127$ are all prime. But

$$2^{11} - 1 = 2047 = 23 \times 89,$$

so the answer is $p = 11$.

(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 $q \equiv 1 \pmod{p}$.

Solution: Certainly q is odd (being a divisor of the odd number $2^p - 1$), so $\mathrm{ord}_q(2)$ makes sense. As seen in lectures and previous exercises, the sequence of residues of 2^n modulo q is periodic with period $\mathrm{ord}_q(2)$, and in particular $2^n \equiv 1 \pmod{q}$ if and only if n is a multiple of $\mathrm{ord}_q(2)$. But we are given that q divides $2^p - 1$, which means that $2^p \equiv 1 \pmod{q}$. Hence p is a multiple of $\mathrm{ord}_q(2)$, and since p is prime and $\mathrm{ord}_q(2) > 1$ (clearly), this forces $\mathrm{ord}_q(2) = p$. Now Fermat's Little Theorem tells us that $2^{q-1} \equiv 1 \pmod{q}$, so $q - 1$ is a multiple of $\mathrm{ord}_q(2) = p$, which means that $q \equiv 1 \pmod{p}$.

This restriction on the factors of $2^p - 1$ makes it easier to check whether or not $2^p - 1$ is prime than it is to check other odd numbers of similar size. For this reason, the largest numbers known to be prime are all Mersenne primes.

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.

Solution: The most obvious such value is $n = 41$: $41^2 + 41 + 41$ is obviously a multiple of 41. Slightly less obvious is $n = 40$: $40^2 + 40 + 41 = 40 \times 41 + 41$ is also a multiple of 41 (in fact it is $41^2 = 1681$). Remarkably, for every n between 0 and 39, $n^2 + n + 41$ is prime: the primes involved are 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 and 1601.

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

Solution: We need to check that this set does not contain two representatives from the same residue class. Since it has exactly m elements, that

would imply that it contains exactly one representative from each residue class. Indeed, assume we have

$$2n \equiv 2n' \pmod{m}, \quad 1 \leq n, n' \leq m.$$

Since m is odd, we can cancel 2 from both sides to get $n \equiv n' \pmod{m}$. That is only possible if $n = n'$.

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

Solution: The map $a \to a^2 \pmod{m}$ does not give a bijection if $m > 2$: we have $1 \not\equiv -1 \pmod{m}$ but $1^2 = (-1)^2$, hence the map is not injective, and so the set $\{a^2 \mid 0 \leq a < m\}$ is of cardinality $< m$. In particular, this set cannot form a *complete* set of residues modulo m (which always has cardinality m).
⟦Why does this argument not work for $m = 2$?⟧

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

Solution: The sequence of residues of powers of 2 modulo 89 is:

$$1, 2, 4, 8, 16, 32, 64, 39, 78, 67, 45, 1, \ldots$$

So $\mathrm{ord}_{89}(2) = 11$ (a divisor of $89-1$, in accordance with Fermat's Little Theorem).

The sequence of residues of powers of 3 modulo 17 is:

$$1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1, \ldots$$

So $\mathrm{ord}_{17}(3) = 16$ (the maximum possible order modulo 17, according to Fermat's Little Theorem).

The sequence of residues of powers of 10 modulo 37 is simply $1, 10, 26, 1, \ldots$. So $\mathrm{ord}_{37}(10) = 3$.

***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 $k \in \mathbb{N}$.

Solution: We can show this by proving the contrapositive assertion: if a is a positive integer which is not a power of 2, then $2^a + 1$ is composite. The fact that a is not a power of 2 means that it has some odd divisor m which is bigger than 1; say $a = mb$, where $1 \leq b < a$. Then setting $x = 2^b$ in the factorization identity gives

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

Since $1 \leq b < a$ we have $3 = 2^1 + 1 \leq 2^b + 1 < 2^a + 1$, so $2^b + 1$ is a nontrivial divisor of $2^a + 1$, proving that $2^a + 1$ is composite.

(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:

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

Solution: Since $5\times 2^7 \equiv -1 \pmod{641}$, it follows that

$$5^4\times 2^{28} = (5\times 2^7)^4 \equiv (-1)^4 \pmod{641}.$$

That is, $5^4\times 2^{28}\equiv 1 \pmod{641}$. But also $5^4\equiv -2^4 \pmod{641}$; so

$$1\equiv 5^4\times 2^{28}\equiv -2^4\times 2^{28} = -2^{32} \pmod{641},$$

which shows that 641 divides $2^{32}+1$.

****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.

Solution: Here is a rough idea of one argument. The details involved in making this precise are details of analysis rather than of number theory, so it seems justifiable to omit them for the purposes of this course.

Let d and N be positive integers with $d\le N$. Let $P(d,N)$ denote the probability that two independently randomly chosen elements $a,b\in\{1,2,\cdots,N\}$ satisfy $\gcd(a,b)=d$. We want to show that

$$\lim_{N\to\infty} P(1,N) = \frac{6}{\pi^2}.$$

One obvious fact is that

$$\sum_{d=1}^{N} P(d,N) = 1,$$

because our elements a,b do have some uniquely defined gcd. We want to relate $P(d,N)$ for $d>1$ to $P(1,N')$ for some N', so that this obvious fact will imply something about $P(1,N')$.

Note that the number of multiples of d in the set $\{1,2,\cdots,N\}$ is $\lfloor \frac{N}{d}\rfloor$ (the greatest integer less than or equal to $\frac{N}{d}$). So the probability that a randomly chosen integer $a\in\{1,2,\cdots,N\}$ is a multiple of d is $\frac{1}{N}\lfloor\frac{N}{d}\rfloor$. This probability is "approximately $\frac{1}{d}$" in a fairly strong sense: it equals $\frac{1}{d}$ exactly if N is a multiple of d, and tends to $\frac{1}{d}$ in the limit as $N\to\infty$ (because the difference $\frac{N}{d}-\lfloor\frac{N}{d}\rfloor$ is bounded above by 1, so it becomes negligible when multiplied by $\frac{1}{N}$).

Now $\gcd(a,b) = d$ is equivalent to the following three conditions: (i) a is a multiple of d, (ii) b is a multiple of d, (iii) $\gcd(a/d, b/d) = 1$. It is clear that (i) and (ii) are independent events, so the probability of both of them occurring is $(\frac{1}{N}\lfloor\frac{N}{d}\rfloor)^2$, which is "approximately $\frac{1}{d^2}$" in the same sense explained above. Assuming both (i) and (ii), we can treat a/d and b/d as independently randomly chosen elements of $\{1, 2, \cdots, \lfloor\frac{N}{d}\rfloor\}$, so the probability that (iii) occurs is $P(1, \lfloor\frac{N}{d}\rfloor)$. We conclude that

$$P(d,N) = \left(\frac{1}{N}\left\lfloor\frac{N}{d}\right\rfloor\right)^2 P\left(1, \left\lfloor\frac{N}{d}\right\rfloor\right).$$

Substituting into the "obvious fact", we get that

$$\sum_{d=1}^{N}\left(\frac{1}{N}\left\lfloor\frac{N}{d}\right\rfloor\right)^2 P\left(1, \left\lfloor\frac{N}{d}\right\rfloor\right) = 1.$$

By bounding the error in the above approximation, one can deduce that, if we replaced $(\frac{1}{N}\lfloor\frac{N}{d}\rfloor)^2$ by $\frac{1}{d^2}$ in this equation, it would still be true as a statement about the limit as $N \to \infty$. In other words, one can deduce that

$$\lim_{N\to\infty}\sum_{d=1}^{N}\frac{1}{d^2}P\left(1, \left\lfloor\frac{N}{d}\right\rfloor\right) = 1.$$

Note that the dominant terms in the sum over d are those where d is small, so that the factor $\frac{1}{d^2}$ is not too small: these are the terms containing a factor $P(1, N')$ where N' is comparable to N in size. With more careful error bounding, one can deduce from such considerations that

$$\left(\lim_{N\to\infty}\sum_{d=1}^{N}\frac{1}{d^2}\right)\left(\lim_{N\to\infty}P(1,N)\right) = 1.$$

Since we are given that the first limit on the left-hand side equals $\dfrac{\pi^2}{6}$, the second limit must equal $\dfrac{6}{\pi^2}$.