The University of Sydney
School of Mathematics and Statistics

Solutions to Tutorial 1 (Week 2)

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. Write down the (positive integer) divisors of 28 in increasing order; you should find that there are six of them. Observe that they can be grouped into three pairs where the two numbers in each pair multiply together to give 28. Bearing this in mind, which positive integers n have an odd number of divisors?

Solution: The divisors of 28 are:

$$1,\ 2,\ 4,\ 7,\ 14,\ 28.$$

As the question noted, these fall into three pairs, each pair multiplying together to give 28: namely, $\{1, 28\}$, $\{2, 14\}$, and $\{4, 7\}$. This was inevitable, because if d is a (positive) divisor of a positive integer n (such as 28), then so is n/d. So the divisors of n always occur in pairs $\{d, n/d\}$, **except** that there is one case where we can't call $\{d, n/d\}$ a "pair", which is if $d = n/d$. This equality implies that $n = d^2$ is a perfect square, i.e. $n \in \{1, 4, 9, 16, 25, \cdots\}$. The conclusion is: if n is not a perfect square, then the divisors of n can be grouped into pairs $\{d, n/d\}$, and hence n has an even number of divisors; if n is a perfect square, then the divisors of n can be grouped into pairs $\{d, n/d\}$ **except** for the divisor $\sqrt{n}$ which is on its own, and hence n has an odd number of divisors.

2. In each case, use the Euclidean Algorithm to find the greatest common divisor $\gcd(a, b)$.

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

Solution: Applying the Euclidean Algorithm, we have:

$$35 = 2 \times 14 + 7$$
$$14 = 2 \times 7 + 0$$

So $\gcd(35, 14) = 7$, the last nonzero remainder that appears on the right-hand side. (With numbers as small as this, one could certainly work out their greatest common divisor without the Euclidean Algorithm, especially if one knows their prime factorizations. But going through the steps of the Euclidean Algorithm is useful for answering the next question.)

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

Solution: Applying the Euclidean Algorithm, we have:

$$\begin{aligned} 168 &= 1 \times 132 + 36 \\ 132 &= 3 \times 36 + 24 \\ 36 &= 1 \times 24 + 12 \\ 24 &= 2 \times 12 + 0 \end{aligned}$$

So $\gcd(168, 132) = 12$.

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

Solution: Applying the Euclidean Algorithm, we have:

$$\begin{aligned} 847 &= 1 \times 510 + 337 \\ 510 &= 1 \times 337 + 173 \\ 337 &= 1 \times 173 + 164 \\ 173 &= 1 \times 164 + 9 \\ 164 &= 18 \times 9 + 2 \\ 9 &= 4 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

So $\gcd(847, 510) = 1$.

3. For each of the pairs a, b in the previous question, find integers s, t such that $\gcd(a, b) = sa + tb$.

Solution: The information required to find s, t is all contained in the steps of the Euclidean Algorithm carried out in each part of the previous question.

For part (a), the very first line of the Euclidean Algorithm calculation says $35 = 2 \times 14 + 7$, which can be rearranged to $7 = 35 - 2 \times 14 = a - 2b$. So $s = 1$, $t = -2$ is one solution. Note that this is not the only solution: for instance, $s = -1$, $t = 3$ is another solution. In fact, from results in lectures it follows that a general solution is $s = 1 + 2u$, $t = -2 - 5u$ where u is an arbitrary integer.

For part (b), one can find a solution by rearranging each of the steps of the Euclidean Algorithm calculation, and thus successively expressing in the form $sa + tb$ each of the nonzero remainders 36, 24, and 12, the last of which is $\gcd(168, 132)$:

$$\begin{aligned} 36 &= 168 - 132 = a - b, \\ 24 &= 132 - 3 \times 36 = b - 3(a - b) = -3a + 4b, \\ 12 &= 36 - 24 = (a - b) - (-3a + 4b) = 4a - 5b. \end{aligned}$$

So one solution (again, not unique) is $s = 4$, $t = -5$.

For part (c) the same method would work, but with so many steps in the Euclidean Algorithm, setting it out in the same way as part (b) would be long and perhaps conducive to error. A more concise way to set out the calculation is to use the extended Euclidean Algorithm explained in lectures, which simultaneously finds $\gcd(a, b)$ and integers s, t such that $\gcd(a, b) = sa + tb$. This involves constructing

a table, which initially consists of the given numbers a and b and the numbers 0, 1, 1 and 0, laid out as follows:

$$\begin{array}{cc} 847 & 510 \\ \\ 0 & 1 \\ 1 & 0\,. \end{array}$$

There are four rows; the second one is blank initially. We proceed to extend the table to the right, one column at a time, using rules described below, and stop when we get 0 in the top row. In this example, the final table is as follows:

$$\begin{array}{ccccccccc} 847 & 510 & 337 & 173 & 164 & 9 & 2 & 1 & 0 \\ & & 1 & 1 & 1 & 1 & 18 & 4 & 2 \\ 0 & 1 & 1^- & 2 & 3^- & 5 & 93^- & 377 & \\ 1 & 0 & 1 & 1^- & 2 & 3^- & 56 & 227^- & . \end{array}$$

The answer is that the greatest common divisor of a and b is the last nonzero number in the top row (which is 1 in this example) while s and t are respectively the numbers below the gcd in the 4th and 3rd rows, except that one of these has to be replaced by its negative. Which one is replaced by its negative depends on whether the process completed in an odd number of steps or an even number of steps; we keep track of this with a little minus sign that alternates between the 3rd and 4th rows. In this example the answer is that $s = -227$ and $t = 377$. We can check that

$$(-227) \times 847 + 377 \times 510 = -192269 + 192270 = 1.$$

The rules for extending the table are as follows. Suppose we are part way through; call the last two numbers in the first row A and B, the last two in the third row L and K, the last two in the fourth row N and M. Divide B into A and let the quotient be Q and the remainder R. Then the four numbers to go in the next column are R, Q, $QK + L$ and $QM + N$.

$$\begin{array}{cc|c} A & B & R \\ \cdots & \cdots & Q \\ L & K & QK + L \\ N & M & QM + N\,. \end{array}$$

If we had done parts (a) and (b) the same way, the final tables would be as follows:

$$\begin{array}{cccc} 35 & 14 & 7 & 0 \\ & & 2 & 2 \\ 0 & 1 & 2^- & \\ 1 & 0 & 1 & \end{array}\,, \qquad \begin{array}{cccccc} 168 & 132 & 36 & 24 & 12 & 0 \\ & & 1 & 3 & 1 & 2 \\ 0 & 1 & 1^- & 4 & 5^- & \\ 1 & 0 & 1 & 3^- & 4 & \end{array}\,.$$

4. Find the prime factorizations of 2016 and 2068. (Simple trial division will work.)

Solution: Since 2016 is obviously even, we can start by taking out factors of 2:

$$2016 = 2 \times 1008 = 2^2 \times 504 = 2^3 \times 252 = 2^4 \times 126 = 2^5 \times 63.$$

Now $63 = 3^2 \times 7$, so the prime factorization of 2016 is $2^5 \times 3^2 \times 7$. Similarly,

$$2068 = 2^2 \times 517 = 2^2 \times 11 \times 47.$$

To find the factorization of 517, the easiest way seems to be simple trial division: we can check easily that 3 and 7 don't divide 517, and 11 does, leaving 47 as a quotient. If you didn't already know that 47 was prime, it would follow from the calculations already done: the only primes less than $\sqrt{47}$ are 2, 3 and 5, and we saw that none of these divides $517 = 11 \times 47$, so they can't divide 47 either.

5. Use Fermat's factorization method to factorize 629 and 3139.

Solution: In Fermat's method of factorizing an odd integer n, we try to find an integer m such that $m^2 - n$ is a perfect square. Take $n = 629$. We have $25^2 = 625 < 629 < 26^2$, so the first value of m to try is 26:

$$26^2 - 629 = 676 - 629 = 47, \text{ not a square.}$$
$$27^2 - 629 = 729 - 629 = 100, \text{ a square.}$$

So $629 = 27^2 - 10^2 = (27 - 10)(27 + 10) = 17 \times 37$. Both 17 and 37 are prime, so this is the prime factorization of 629. If we had used naive trial division, we would have had to test whether 3, 7, 11 and 13 divided 629 before having success with 17, so it probably would have taken longer.

Now take $n = 3139$. We have $56^2 = 3136 < 3139 < 57^2$, so the first value of m to try is 57:

$$57^2 - 3139 = 3249 - 3139 = 110, \text{ not a square.}$$
$$58^2 - 3139 = 3364 - 3139 = 225, \text{ a square.}$$

So $3139 = 58^2 - 15^2 = (58 - 15)(58 + 15) = 43 \times 73$. Both 43 and 73 are prime, so this is the prime factorization of 3139.

***6.** (a) Suppose that $a = qb$, with $a, b, q \in \mathbb{Z}^+$. Show that $2^b - 1$ divides $2^a - 1$.

Solution: Setting $x = 2^b$ in the factorization identity

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

gives

$$2^a - 1 = (2^b - 1)(2^{b(q-1)} + 2^{b(q-2)} + \cdots + 2^b + 1),$$

which shows that $2^b - 1$ divides $2^a - 1$.

(b) Hence show that if a is a composite number, then so is $2^a - 1$.

Solution: If a is composite, then we can write $a = qb$ where $q, b > 1$. By the previous part, $2^b - 1$ divides $2^a - 1$. Since $1 < b < a$, we have $1 = 2^1 - 1 < 2^b - 1 < 2^a - 1$. So $2^a - 1$ has a nontrivial divisor and is therefore composite.

(c) Now suppose that $a = qb + r$, with $a, b, q \in \mathbb{Z}^+$ and $0 \leq r < b$, so that r is the residue of a modulo b. Show that $2^r - 1$ is the residue of $2^a - 1$ modulo $2^b - 1$.

Solution: Certainly $0 \leq 2^r - 1 < 2^b - 1$, so it is enough to show that $2^a - 1 = Q(2^b - 1) + (2^r - 1)$ for some integer Q. In other words, it is enough to show that $2^b - 1$ divides

$$(2^a - 1) - (2^r - 1) = 2^{qb+r} - 2^r = 2^r(2^{qb} - 1).$$

But by the first part, $2^b - 1$ divides $2^{qb} - 1$, so it certainly divides $2^r(2^{qb} - 1)$.

(d) Bearing the Euclidean Algorithm in mind, show that for any positive integers a, b we have $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.

Solution: Suppose that the Euclidean Algorithm applied to a and b generates the sequence r_0, r_1, r_2, $\ldots$, $r_m = 0$. These numbers are just obtained by successively taking residues of certain divisions. So by the result proved in the previous part, the Euclidean Algorithm applied to $2^a - 1$ and $2^b - 1$ will generate the sequence $2^{r_0} - 1$, $2^{r_1} - 1$, $2^{r_2} - 1$, $\ldots$, $2^{r_m} - 1 = 0$. So $\gcd(2^a - 1, 2^b - 1) = 2^d - 1$, where $d = r_{m-1} = \gcd(a, b)$.

Extra Exercises:

7. Find the prime factorization of 2017.

Solution: It turns out that 2017 is prime. Using trial division, one can verify this by checking that 2017 is not divisible by any of the primes less than $\sqrt{2017}$, namely:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43.$$

8. Let k be a positive integer and p a prime. Find a formula for the sum of all the (positive integer) divisors of p^k.

Solution: The divisors of p^k are 1, p, p^2, $\ldots$, p^k, and using the formula for the sum of a geometric progression, we find that the sum of the divisors of p^k is $(p^{k+1} - 1)/(p - 1)$.

*__9.__ Use the identity

$$(x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2) = x^4 + 4y^4$$

to determine all pairs of positive integers n, m such that $n^4 + 4m^4$ is prime.

Solution: Suppose that n and m are positive integers such that $n^4 + 4m^4$ is prime. By the given identity, $n^4 + 4m^4$ can be factorized as the product of the two integers $n^2 - 2nm + 2m^2$ and $n^2 + 2nm + 2m^2$. If a prime number p factorizes as ab (with $a, b \in \mathbb{Z}$) then we must have $a = 1$ and $b = p$ or $a = -1$ and $b = -p$ or $a = p$ and $b = 1$ or $a = -b$ and $p = -1$. In the present case, $n^2 + 2nm + 2m^2$ is clearly positive and larger than $n^2 - 2nm + 2m^2$, so we must have $n^2 - 2nm + 2m^2 = 1$. This can be rewritten as $(n - m)^2 + m^2 = 1$, which forces $n - m = \pm 1$ and $m = 0$ or $n - m = 0$ and $m = \pm 1$. The former alternative gives $n = 1$ and $m = 0$, and $n^4 + 4m^4 = 1$ is not a prime number. The latter alternative gives $n = m = 1$, and $n^4 + 4m^4 = 5$, which is prime, so this is the unique solution.

**__10.__ Suppose we want to factorize $n = 10875593$. It turns out that, if we were to apply Fermat's method naively, it would take a long search before we found our desired m such that $m^2 - n$ is a square. However, we might notice as we carried out that search (presumably with the help of a calculator or MAGMA) that

$$3306^2 - n = 11 \times 17^3,$$
$$3834^2 - n = 11^3 \times 13^2 \times 17.$$

Neither of these right-hand sides is a square, as you can tell from the odd exponents, but their product is a square:

$$(3306^2 - n)(3834^2 - n) = 11^4 \times 13^2 \times 17^4 = (11^2 \times 13 \times 17^2)^2.$$

Use this information (and your calculator) to find a nontrivial divisor of n.

Solution: The given equation can be rearranged to put all the n's on the right-hand side:

$$3306^2 \times 3834^2 - (11^2 \times 13 \times 17^2)^2 = n(3306^2 + 3834^2 - n).$$

So we deduce that n divides the left-hand side, which is a difference of two squares and hence factorizes as

$$(3306 \times 3834 - 11^2 \times 13 \times 17^2)(3306 \times 3834 + 11^2 \times 13 \times 17^2).$$

For all we know at this point it may be that one of these two factors is divisible by n and the other is coprime to n, but if n has a nontrivial factorization it is significantly more likely that the prime factors of n are shared between $3306 \times 3834 - 11^2 \times 13 \times 17^2$ and $3306 \times 3834 + 11^2 \times 13 \times 17^2$. So if we find the gcd of n and $3306 \times 3834 - 11^2 \times 13 \times 17^2 = 12220607$, there is a good chance that the result will be a nontrivial divisor of n.

When we apply the Euclidean Algorithm to 12220607 and 10875593 ($= n$), the sequence of remainders we obtain is 1345014, 115481, 74723, 40758, 33965, 6793, 0. Hence 6793 is a nontrivial divisor of 10875593.

In fact, it turns out that the prime factorization of $n = 10875593$ is 1601×6793. So using trial division alone to factorize n, one would have to go up to the prime 1601 before having success; and using Fermat's method alone, one would have to go from $m = \sqrt{n} \approx 3298$ to $m = \frac{1}{2}(6793 + 1601) = 4197$ before having success. This question illustrates the benefits of a hybrid method, invented in 1981 by J. D. Dixon of Carleton University, Canada, where one looks not just for a single number m such that $m^2 - n$ is a square but for a collection of numbers $m_1, \cdots, m_k$ such that $(m_1^2 - n) \cdots (m_k^2 - n)$ is a square.