EECS 203: Discrete Mathematics
Individual Homework 5 (Winter 2016)

Answer Key

Due: June 3, 2016

1. (4 points) Section 4.3 Problem 54

Solution: Suppose by way of contradiction that q_1 , q_2 , . . . , q_n are the only primes of the form 3k + 2. Notice that this list necessarily includes 2. Let Q = $3q_1q_2q_n - 1$. Notice that neither 3 nor any prime of the form 3k + 2 is a factor of Q. But $Q \geq 3 \cdot 2 - 1 = 5 > 1$, so it must have prime factors. Therefore all of its prime factors are of the form 3k + 1. However, the product of numbers of the form 3k + 1 is again of that form, because $(3k + 1)(3l + 1) = 3(3kl + k + l) + 1$. Patently Q is not of that form, and we have a contradiction, which completes the proof.

2. (2 points) Section 4.4 Problem 6 (c)

Solution:

c) We need to find s and t such that $144s + 233t = 1$. Then clearly s will be the desired inverse, since $144s \equiv 1 \mod 233$ (i.e., $144s - 1 = -233t$ is divisible by 233). To do so, we proceed as in Example 2.

Euclidean algorithm computation that gcd(144, 233) = 1:
233 = 144 + 89
144 = 89 + 55
89 = 55 + 34
55 = 34 + 21
34 = 21 + 13
21 = 13 + 8
13 = 8 + 5
8 = 5 + 3
5 = 3 + 2
3 = 2 + 1

Then we reverse our steps and write 1 as the desired linear combination:
$1 = 3 - 2$
$= 3 - (5 - 3) = 2 \cdot 3 - 5$

$= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5$
$= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13$
$= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13$
$= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34$
$= 13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34$
$= 13 \cdot 55 - 21 \cdot (89 - 55) = 34 \cdot 55 - 21 \cdot 89$
$= 34 \cdot (144 - 89) - 21 \cdot 89 = 34 \cdot 144 - 55 \cdot 89$
$= 34 \cdot 144 - 55 \cdot (233 - 144) = 89 \cdot 144 - 55 \cdot 233$

Thus s = 89, so an inverse of 144 modulo 233 is 89, since $144 \cdot 89 = 12816 \equiv 1 \mod 233$.

3. (1 point) Section 4.4 Problem 34

Solution: Fermat's little theorem tells us that $23^{40} \equiv 1 \mod 41$. Therefore $23^{1002} = (23^{40})^{25} \cdot 23^2 \equiv 1^{25} \cdot 529 = 529 \equiv 37 \mod 41$.

4. (2 points) Section 4.4 Problem 36

Solution: By Exercise 35, an inverse of 5 modulo 41 is 5^{39}. This could be calculated using modular exponentiation (or, from a practical point of view, with computer algebra software). The simplest form of this is 33, and it is easy to check that $5 \cdot 33 = 165 \equiv 1 \mod 41$.

5. (2 points) Section 4.4 Problem 50 (b,c,g,h)

Solution: We could use the technique shown in the proof of Theorem 2 to solve each part, or use the approach in our solution to Exercise 32, but since there are so many to do here, it is simpler just to write out all the representations of 0 through 27 and find those given in each part. This task is easily done, since the pattern is clear:

0 = (0, 0)	7 = (3, 0)	14 = (2, 0)	21 = (1, 0)
1 = (1, 1)	8 = (0, 1)	15 = (3, 1)	22 = (2, 1)
2 = (2, 2)	9 = (1, 2)	16 = (0, 2)	23 = (3, 2)
3 = (3, 3)	10 = (2, 3)	17 = (1, 3)	24 = (0, 3)
4 = (0, 4)	11 = (3, 4)	18 = (2, 4)	25 = (1, 4)
5 = (1, 5)	12 = (0, 5)	19 = (3, 5)	26 = (2, 5)
6 = (2, 6)	13 = (1, 6)	20 = (0, 6)	27 = (3, 6)

Now we can read off the answers.

b) 21

c) 1

g) 14

h) 19

6. (3 points) Use RSA to encode the following message where n=(73*83) and e=13 following the scheme in example 8. The message is FAZE. Show your work.

Solution:

$$C_1 = M_1^e = (F * 100 + A)^{13} = (500)^{13} \equiv 4208 \mod 73 * 83$$

$$C_2 = M_2^e = (Z * 100 + E)^{13} = (2504)^{13} \equiv 5015 \mod 73 * 83$$

7. (5 points) Now decode the above message. Again, clearly show your work.

Solution: First, we need to find $d \equiv e^{-1} \mod 72 * 82$. To do this, we will apply the extended euclidean algorithm to write gcd(e,72*82)=1 as a linear combination of e=13 and 72*82=5904

$$\begin{aligned} 5904 &= 454 * 13 + 2 \\ 13 &= 6 * 2 + 1 \\ 2 &= 2 * 1 + 0 \end{aligned}$$

Now, we go back up writing the remainder in terms of the other terms:

$$\begin{aligned} 1 &= 13 - 6 * 2 \\ &= 13 - 6 * (5904 - 454 * 13) \quad = 2725 * 13 - 6 * 5904 \end{aligned}$$

Taking $1 = 2725 * 13 - 6 * 5904 \mod 5904$ gives us $1 \equiv 2725 * 13 \mod 5904$, or in other words, $d = e^{-1} = 13^{-1} = 2725 \mod 5904$

Finally, we compute

$$M_1 = C_1^d = 4208^{2725} \equiv 500 = 5 * 100 + 0 = F * 100 + A \mod 73 * 83$$

$$M_2 = C_2^d = 5015^{2725} \equiv 2504 = 25 * 100 + 4 = Z * 100 + E \mod 73 * 83$$

8. (4 points) Section 5.1 Problem 12

Solution: We proceed by mathematical induction. The basis step (n = 0) is the statement that $(-1/2)^0 = (2+1)/(3 \cdot 1)$, which is the true statement that $1 = 1$. Assume the inductive hypothesis, that

$$\sum_{j=0}^{k} \left(-\frac{1}{2}\right)^j = \frac{2^{k+1} + (-1)^k}{3 \cdot 2^k}$$

We want to prove that

$$\sum_{j=0}^{k+1} \left(-\frac{1}{2}\right)^j = \frac{2^{k+2} + (-1)^{k+1}}{3 \cdot 2^{k+1}}$$

Split the summation into two parts, apply the inductive hypothesis, and do the algebra:

$$\begin{aligned} \textstyle\sum_{j=0}^{k+1} \left(-\frac{1}{2}\right)^j &= \textstyle\sum_{j=0}^{k} \left(-\frac{1}{2}\right)^j + \left(-\frac{1}{2}\right)^{k+1} \\ &= \frac{2^{k+1}+(-1)^k}{3 \cdot 2^k} + \frac{(-1)^{k+1}}{2^{k+1}} \\ &= \frac{2^{k+2}-2(-1)^{k+1}}{3 \cdot 2^{k+1}} + \frac{3(-1)^{k+1}}{3 \cdot 2^{k+1}} \\ &= \frac{2^{k+2}+(-1)^{k+1}}{3 \cdot 2^{k+1}} \end{aligned}$$

9. (4 points) Section 5.1 Problem 18

Solution:

a) Plugging in n = 2, we see that P(2) is the statement $2! < 22$.

b) Since $2! = 2$, this is the true statement $2 < 4$.

c) The inductive hypothesis is the statement that $k! < k^k$.

d) For the inductive step, we want to show for each $k \geq 2$ that P(k) implies P(k + 1). In other words, we want to show that assuming the inductive hypothesis (see part (c)) we can prove that $(k+1)! < (k+1)^{k+1}$.

e) $(k+1)! = (k+1)k! < (k+1)k^k < (k+1)(k+1)^k = (k+1)^{k+1}$

f) We have completed both the basis step and the inductive step, so by the principle of mathematical induction, the statement is true for every positive integer n greater than 1.

10. (3 points) Section 5.1 Problem 32

Solution: The statement is true for the base case, n = 0, since $3|0$. Suppose that $3|(k^3 + 2k)$. We must show that $3|((k+1)^3 + 2(k+1))$. If we expand the expression in question, we obtain $k^3 + 3k^2 + 3k + 1 + 2k + 2 = (k^3 + 2k) + 3(k^2 + k + 1)$. By

the inductive hypothesis, 3 divides $k^3 + 2k$, and certainly 3 divides $3(k^2 + k + 1)$, so 3 divides their sum, and we are done.