18.781 Problem Set 4 Solutions

1. I have made a toy RSA encryption system. I announce to you the public modulus $m = 221$ and the public encryption key $k = 77$. To encrypt a message a to me (which can be any positive number between 1 and 220), you must calculate $a^{77} \pmod{221}$.

1(a). Suppose that you wish to send me the private message 2. What is the encrypted message you should send?

Make a table of the powers-of-two powers of a modulo 221 using by repeated squaring:

$$2^{2^0} \equiv 2 \pmod{221}, \quad 2^{2^1} \equiv 2^2 \equiv 4 \pmod{221}, \quad 2^{2^2} \equiv 4^2 \equiv 16 \pmod{221},$$

$$2^{2^3} \equiv 16^2 \equiv 35 \pmod{2}$$

$$2^{2^4} \equiv 35^2 \equiv 120 \pmod{221}, \quad 2^{2^5} \equiv 120^2 \equiv 35 \pmod{221},$$

$$2^{2^6} \equiv 35^2 \equiv 120 \pmod{221}.$$

Now you can calculate

$$2^{77} \equiv 2^{64} \cdot 2^8 \cdot 2^4 \cdot 2^1 \equiv 120 \cdot 35 \cdot 16 \cdot 2 \equiv 32.$$

1(b). Not content with the ability to send me private messages, you have decided to try to *read* my private messages. You find that the Dean has sent me the encrypted message 95. What was the Dean's actual message to me?

The easiest approach is to invert the key 77 modulo $\phi(221)$. To calculate that, we need to factor 221. Since its square root is smaller than 15, 221 must have a prime factor less than 15. This is a case for trial division. Clearly it isn't divisible by 2, 3, or 5, and the remainder on division by 7 is four. The remainder on division by 11 is 1. It's divisible by 13:

$$221 = 13 \cdot 17,$$

and 17 is also prime. Follows that

$$\phi(221) = (13-1) \cdot (17-1) = 12 \cdot 16 = 192.$$

To decode the message, we must find an inverse of the key 77 modulo 192. I won't go through the Euclidean algorithm method, but it discovers the equation

$$(-2) \cdot (192) + (5) \cdot (77) = 1,$$

so the inverse is 5. To decode a message, raise it to the fifth power modulo 221. For the coded message you sent in (a), this gives

$$32^{2^0} \equiv 32 \pmod{221}, \qquad 32^2 = 1024 \equiv 140 \pmod{221},$$

$$(32^2)^2 \equiv (140)^2 \equiv 152 \pmod{221}.$$

Now

$$32^5 = 32^4 \cdot 32 \equiv 152 \cdot 32 \equiv 2 \pmod{221},$$

which is indeed the secret message you encoded in (a).

For the Dean's message, we compute powers of 95 modulo 221:

$$(95)^{2^0} \equiv 95 \pmod{221}, \qquad 95^2 \equiv 185 \pmod{221},$$

$$(95)^4 \equiv (185)^2 \equiv 191 \pmod{221}.$$

Now we can decode:

$$(95)^5 = (95)^4 \cdot 95 \equiv 191 \cdot 95 \equiv 23 \pmod{221}.$$

The Dean's message was **23**.

2. Recall that Euler's ϕ function is defined for every positive integer m as

$$\phi(m) = \textbf{number of integers } 1 \le a \le m \textbf{ such that } \gcd(a,m) = 1.$$

In particular, this means that $\phi(1) = 1$.

2(a). Suppose that d is a positive divisor of m, and that $1 \le a \le m$. Prove that $\gcd(a,m) = d$ if and only if $d|a$ and $\gcd(a/d, m/d) = 1$.

If $\gcd(a,m) = d$, then first of all $d|a$ and (as we were already assuming) $d|m$. Therefore $\gcd(a/d, m/d) = x$ is defined; it is the largest positive integer dividing both a/d and m/d. Now it's clear that $z|(a/d)$ if and only if $(zd)|a$. (This is written in Theorem 1.1(6) of the text.) So xd is the largest integer dividing a and m.

2(b). Suppose that d is a positive divisor of m. Prove that

$$\phi(m/d) = \textbf{number of integers } 1 \le a \le m \textbf{ such that } \gcd(a,m) = d.$$

By(a), the set on the right is

$$\text{integers } 1 \le a \le m \text{ such that } \gcd(a/d, m/d) = 1.$$

That is, it is the same as d times the integers

$$\text{integers } 1 \le b \le m/d \text{ such that } \gcd(b, m/d) = 1.$$

The number of such integers is $\phi(m/d)$ by definition.

2(c). Prove Gauss's formula

$$\sum_{d|m} \phi(m/d) = m.$$

If $1 \le a \le m$, then $\gcd(a,m)$ must be a positive divisor d of m. By (a), the m integers from 1 to m break into disjoint sets

$$S_d =_{\text{def}} \{1 \le a \le m \mid \gcd(a,m) = d\}.$$

Since these sets are disjoint,

$$m = \sum_{d|m} \#S_d.$$

By (b), this is exactly Gauss's formula.

2(d). You know that if p is a prime number, then $\phi(p) = p - 1$. Use this fact and part (c) to calculate $\phi(21)$.

If $m = pq$ has distinct prime factors p and q, then the divisors of pq are 1, p, q, and pq. Gauss's formula is therefore

$$pq = \phi(pq) + \phi(p) + \phi(q) + \phi(1) = \phi(pq) + (p - 1) + (q - 1) + 1.$$

Therefore

$$\phi(pq) = pq - p - q + 1 = (p - 1)(q - 1).$$

In particular,

$$\phi(21) = \phi(3 \cdot 7) = (3 - 1)(7 - 1) = \mathbf{12}.$$

3. This problem is stolen from a text "Discrete math for computer science students" by Ken Bogart and Cliff Stein. The goal is to factor $N = 224,551$, in order to get some sense of how difficult factoring large numbers might really be. You may assume (as you might verify by trial divisions by hand) that N has no prime factors less than or equal to 59. You may also assume (as you might verify with a calculator) that $N^{1/2} = 473.86\ldots$ and $N^{1/3} = 60.78\ldots$.

3(a). Prove that if N is not prime, then it must be the product of exactly two prime factors $p_1 < p_2$, with $61 \leq p_1 \leq 467$.

Assume to the contrary that N is the product of three or more primes. Pick three of those primes, p_i for $i = 1, 2, 3$. We are given that $p_i > 59$ for all i. As the p_is are prime, we have $p_i \geq 61 > N^{1/3}$, and hence their product is greater than N, a contradiction. As $N^{1/2}$ is not a natural number, we have that the two prime factors are distinct, say $p_1 < p_2$, and as were given $p_1 > 59$, we must have $p_1 \geq 61$. We also must have $p_1 < N^{1/2}$. We can check (in our prime table, for example) that the largest prime less than 474 is 467.

3(b). Find a table of prime numbers. How many are there between 61 and 467?

In my table they aren't numbered, so I actually had to count; I got **74**, but that's not absolutely reliable.

3(c). Suppose that some kindly oracle tells you that p_1 is between 400 and 450. Use trial divisions (with the table of primes you located in (b)) to find a prime factorization of N.

The result of this effort is $\mathbf{224551 = 431 \cdot 521}$.