18.781 Problem Set 4

Due Monday, October 3 in class.

1. Throughout this problem, n_1 and n_2 are relatively prime natural numbers greater than 1, and $n = n_1 n_2$.

1(a). Show that the decimal expansion of 1/91 has period 6.

1(b). Show that an integer k is divisible by n if and only if k is divisible by n_1 and by n_2.

1(c). Suppose that b and m are any integers. Show that the congruence $b \equiv m \pmod{n}$ holds if and only if the two congruences

$$b \equiv m \pmod{n_1}, \qquad b \equiv m \pmod{n_2}$$

both hold.

1(d). Suppose that $\gcd(a, n) = 1$, that the order of a modulo n_1 is x_1, and that the order of a modulo n_2 is x_2. Show that the order of a modulo n is $\operatorname{lcm}(x_1, x_2)$.

1(e). Find a base a so that the base a expansion of 1/91 has period 4.

2(a). Calculate $11^{60} \pmod{77}$. (Hint: the book suggests computing

$$11^1 \pmod{77}, \qquad 11^2 \pmod{77}, \qquad 11^4 \pmod{77}, \ldots$$

by repeated squaring, then using the binary expansion of 60. This works fine. It's also possible to use some ideas from the first problem above.

2(b). Suppose $n = 77$ and $e = 13$. You can take for granted that $\phi(77) = 60$. Find natural numbers k and d so that

$$ed - k\phi(n) = 1.$$

2(c). In the text's description of RSA, there is on the bottom of page 72 a calculation in symbols n, m, e, and d. Rewrite this calculation using the numbers $n = 77$, $m = 12$, $e = 13$, and d and k found in (b). Comment.

2(d). Explain how to fix the problem you found in (c).

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 $61 \le p_1 \le 467$.

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

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.

4. Prove that 4 is not a primitive root modulo 997.