SOLUTIONS TO HOMEWORK 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 $\frac{1}{91}$ has period 6.

**Ans:** It was shown in class that the period of the decimal expansion of $\frac{1}{m}$ is the same as the order of $10$ modulo $m$. (This is true in general for $\frac{1}{m}$ with $m$ relatively prime to 10.) We calculate:

\[
\begin{align*}
10 &\equiv 10 \pmod{91} \\
10^2 &\equiv 9 \pmod{91} \\
10^3 &\equiv 90 \pmod{91} \\
10^4 &\equiv 81 \pmod{91} \\
10^5 &\equiv 82 \pmod{91} \\
10^6 &\equiv 1 \pmod{91}
\end{align*}
\]

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

**Ans:**

$\Rightarrow$ We assume $k$ is divisible by $n_1$, i.e., that we can write $k = n_1 m$ for some integer $m$. Then $k = n_1(n_2m)$ and $k = n_2(n_1m)$. Hence, $k$ is divisible by $n_1$ and $n_2$.

$\Leftarrow$ Now we assume we have equations $k = n_1 m_1$ and $k = n_2 m_2$. Consider any factor of $n_2$ of the form $p_i^a$. As $n_1$ and $n_2$ are relatively prime, from the uniqueness of factorization into primes and the equation $n_1 m_1 = n_2 m_2$, we have that $p_i^a$ divides the left hand side and that no $p_i$ term divides $n_1$, and hence $p_i^a$ divides $m_1$. The same holds for any factor of $n_2$, and hence $n_2$ divides $m_1$. Say $n_2 k_2 = m_1$. Then $k = n_1 m_1 = n_1 n_2 k_2 = nk_2$.

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

\[
b \equiv m \pmod{n_1}, \quad b \equiv m \pmod{n_2}
\]

both hold.

**Ans:** Straight from the definition of congruence, $b \equiv m \pmod{n}$ if and only if $n$ divides $b - m$. The result now follows immediately from 1(b).

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 $\text{lcm}(x_1, x_2)$.

**Ans:** By part (c), $a^{x_1} \equiv 1 \pmod{n_1}$ if and only if $a^{x_1} \equiv 1 \pmod{n_1}$ for $i = 1, 2$. Thus, $x$ must be a multiple of both $x_1$ and $x_2$, and so the order of $a$ modulo $n$ is the least common multiple of $x_1$ and $x_2$.

1(e). Find a base $a$ so that the base $a$ expansion of $\frac{1}{91}$ has period 4.
Ans: This is analogous to the situation in 1(a), so we want to find a number $a$ such that $a$ is relatively prime to 91 and such that the order of $a$ modulo 91 is 4. One can check that $a = 57$ is such a number. There are probably smaller solutions, but here is an explanation for how that one could naturally be found.

By part (d), since $91 = 7 \times 13$, it suffices to find an element $a$ with orders $x_1$ modulo 7 and $x_2$ modulo 13 such that lcm($x_1, x_2$) = 4. So, either $x_1$ or $x_2$ must equal 4 and the other must equal 1, 2, or 4. To find an element of order 4, we find an element $a'$ such that $(a')^2 \equiv -1 \pmod{7}$ or $(a')^2 \equiv 1 \pmod{13}$. The first such $a'$ is 5: $5^2 = 25 \equiv -1 \pmod{13}$. Now, let’s find $a$ such that $a \equiv 5 \pmod{13}$ and such that $a \equiv \pm 1 \pmod{7}$ (i.e., so that $a$ has order 4 modulo 13 and order 1 or 2 modulo 7.) It’s clear that the first such a is 57.

2(a). Calculate $11^{60} \pmod{77}$. (Hint: the book suggests computing $11^1 \pmod{77}, 11^2 \pmod{77}, 11^4 \pmod{77}, \ldots$ 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.

Ans: From 1(c), we know that $11^{60} \equiv m \pmod{77}$ if and only if $11^{60} \equiv m \pmod{11}$ and $11^{60} \equiv m \pmod{7}$. It’s clear that $11^{60} \equiv 0 \pmod{11}$. And we also have

\[
\begin{align*}
11 &\equiv 4 \pmod{7} \\
11^2 &\equiv 2 \pmod{7} \\
11^3 &\equiv 1 \pmod{7} \\
11^{60} &\equiv (11^3)^{20} \equiv 1 \pmod{7}
\end{align*}
\]

Since $1 \neq 0$, we can’t apply 1(c) directly. What we need to do is find a number which is both congruent to 1 (mod 7) and congruent to 0 (mod 11). It’s clear by inspection that 22 is the smallest such natural number. (The Chinese Remainder Theorem we’ll see later says it’s the only such number mod 77.) Hence, by 1(c), $11^{60} \equiv 22 \pmod{77}$. We want the coefficient of $e$ to be a natural number, so we add $-13 \cdot 60 + 60 \cdot 13 = 0$ to the equation and get $-8 \cdot 60 + 37 \cdot 13 = 1$. Hence, in the notation from the statement of the problem, $d = 37$ and $k = 8$.

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

\[ed - k\phi(n) = 1.\]

Ans: We use, as usual, the Euclidean algorithm, but we will shorten it slightly this time: $60 = 4 \times 13 + 8$ is the first step, as usual. We can find by inspection that $5 \times 8 - 3 \times 13 = 1$. So, plugging the second equation into the first, we have

\[5 \times (60 - 4 \times 13) - 3 \times 13 = 1,
\]

and this is just $5 \times 60 - 23 \times 13 = 1$. We want the coefficient of $e$ to be a natural number, so we add $-13 \cdot 60 + 60 \times 13 = 0$ to the equation and get $-8 \times 60 + 37 \times 13 = 1$. Hence, in the notation from the statement of the problem, $d = 37$ and $k = 8$.

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.

Ans: There was a typo in the statement of the problem which unfortunately changes the result and so this problem will likely not be graded.
SOLUTIONS TO HOMEWORK 4

It’s clear from the wording of the problem, or from the statement of 2(d), that something should go wrong in the calculation. If you look at the four lines of equations at the bottom of page 72, the only step where a non-trivial result is used is the replacement of $m^{\phi(n)}$ with 1. Euler’s Theorem holds whenever $m$ and $n$ are relatively prime, so $m = 12$ will not lead to an error. On the other hand, $m = 11$ (see 2(a)) will. Note that the value of $m$ was not used in 2(b).

We plug in the numbers, with $m = 11$:

$$11^{13 \cdot 37} = 11^{1+8 \cdot 60}$$
$$= 11 \cdot (11^{60})^8$$
$$\equiv 11 \cdot 22^8 \pmod{77}$$

by 2a,

$$\equiv 11 \cdot 22 \pmod{77}$$

because $22^2 \equiv 22 \pmod{77}$,

$$\equiv 11 \pmod{77}.$$ 

So, even though the intermediate steps are different from what is printed in the book, the end result in this particular instance is the same.

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

Ans: We could require that the message and $n$ be relatively prime. You might object that the whole point is that $n$ is hard to factor into primes, but for a given message $m$, it’s easy to check if it’s relatively prime to $n$ (by the Euclidean algorithm).

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 $N^{1/3} = 473.86\ldots$ 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 $61 \leq p_1 \leq 467$.

Ans: 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 $p_i$’s are prime, we have $p_i \geq 61 > N^{1/3}$, and hence their product is greater than $N$, a contradiction.

As the square root is not a natural number, we have that the two prime factors are distinct, say $p_1 < p_2$, and as we’re given $p_1 > 59$, we must have $p_1 \geq 61$. We also must have $p_1 < N^{1/2}$. We can check 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?

Ans: 74 (I hope)

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 $N$. 
Ans: $N = 224, 551 = 431 \times 521$.

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

Ans: From Euler’s Theorem (using the fact that 997 is prime), we have $2^{996} \equiv 1 \pmod{997}$.

Because 996 is even, we have that $4^{498} = 2^{2 \cdot 498} \equiv 1 \pmod{997}$,

and hence 4 is not a primitive root modulo 997.