PROBLEM SET 8: RSA AND PRIME TESTING (DUE NOVEMBER 15)

HARM DERKSEN

Problem 1. Do 31.7-1 in the book.

Solution: We have $\phi(319) = \phi(29 \cdot 11) = 28 \cdot 10 = 280$. We have to find d with $3d \equiv 1(\text{mod} 280)$. Now $280 = 3 \cdot 93 + 1$, so $3 \cdot 93 \equiv -1(\text{mod} 280)$ and $3 \cdot (-93) \equiv 1(\text{mod} 280)$. Take $d = (-93) + 280 = 197$. To encrypt $M = 100$, we compute $100^3 \bmod 319$. Now $100^2 = 31 \cdot 319 + 111$ and $100 \cdot 111 = 11100 = 34 \cdot 319 + 254$. So finally $100^3 \equiv 100 \cdot 111 \equiv 254(\text{mod} 319)$.

Problem 2. Do 31.8-3 in the book.

Solution: If $\gcd(x-1, n) = n$, then $x \equiv 1(\text{mod} n)$. If $\gcd(x-1, n) = 1$, then from $n \mid (x-1)(x+1)$ follows that n divides $x+1$ and $x \equiv -1(\text{mod} n)$. This shows that $\gcd(x-1, n)$ is a nontrivial divisor of n. The prove that $\gcd(x+1, n)$ is a nontrivial divisor goes similarly.

Problem 3. Do 31.9-1 in the book.

Solution: Consider the sequence modulo 73 as in figure 31.7(c) in the book. The first time, the value of y lies within the loop is when y is set to $x_8 = 814$. Then we have $y \equiv 11(\text{mod} 73)$. The loop modulo 73 has length four. We get $x_{12} = 84 \equiv 11(\text{mod} 73)$ again. The computation of $\gcd(y - x_1 2, 1387)$ (where y is set equal to x_8) yields $\gcd(814 - 84, 1387) = 73$. This is the first time that the divisor 73 will be printed. (the divisor 19 will be printed earlier).

Problem 4. * Do 31.8-2 in the book.

Solution: From the formula for $\phi(n)$ it is clear that

$$\lambda(n) = \text{lcm}(\phi(p_1^{e_1}), \ldots, \phi(p_r^{e_r})) \text{ divides } \phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r}).$$

Suppose that a is relatively prime to n. Then a is relatively prime to $p_i^{e_i}$ for all i and

$$a^{\lambda(n)} \equiv 1(\text{mod} p_i^{e_i})$$

because $\lambda(n)$ is divisible by $\phi(p_i^{e_i})$. It follows that $a^{\lambda(n)} - 1$ is divisible by $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = n$ and $a^{\lambda(n)} \equiv 1(\text{mod} n)$. Suppose that $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is Carmichael. Now $p_i^{e_i - 1}$ divides $\phi(p_i^{e_i})$, $\lambda(n)$ and $n - 1$. But $p_i^{e_i - 1}$ also divides n, hence $p_i^{e_i - 1}$ divides $n - (n-1) = 1$. This can only happen when $e_i = 1$ for all i, which means that n is squarefree. Suppose that $n = pq$ with $p < q$

primes. If n is Carmichael then $\lambda(n)$ divides $n-1$, so $p-1$ and $q-1$ divide $n-1$. Write $n-1=a(q-1)$. Clearly $a>p$ because $p(q-1)=n-p<n$. So $n-1\geq(p+1)(q-1)$ which implies that $n-1\geq pq+q-p-1=n-1+(q-p)$. We conclude that $p\geq q$ which contradicts our assumption that $p<q$.