MAT 311: Number Theory
Spring 2006

Solutions to HW7

1. (Davenport, pp.225, ex. 8.06) We would like to find a good linear congruential method for simulating throws of a die. Recall that such a model is of the form $x_{n+1} \equiv ax_n + c \mod m$, provided $a \equiv 1 \mod p$ for every prime p dividing m, $a \equiv 1 \mod 4$ if $4 \,|\, m$, and $(c, m) = 1$. Now, in our case, taking mod 6 would be a big mistake, because to get a sequence of period 6 we would be forced to take the coefficient a of x_n and the constant c to be ± 1 which then would give us a monotonic (*i.e.* increasing or decreasing) sequence (not pseudorandom). So, let's try to work mod 7. Now, a good choice for simulating throws of a die would be $x_{n+1} \equiv 3 \cdot x_n \mod 7$ (observe that 3 is a primitive root mod 7, and taking index to the base 3 will reduce it to a linear congruential method mod 6). So, given seed x_0, the other numbers that are generated are $3x_0, 3^2 x_0, \ldots 3^6 x_0$. For a suitable seed x_0, this set of numbers will trace all the numbers from 1 to 6.

2. (Davenport, p.219, ex. 8.07) We would like to find a good linear congruential method for simulating throws of two dice. The idea is similar. First die will be simulated by the method we used in the first problem above: $x_{n+1} \equiv 3 \cdot x_n \mod 7$. Similarly, for the second die we will choose $y_{n+1} \equiv 5 \cdot y_n \mod 7$ (we cannot take the same coefficient, because otherwise x_n and y_n would be related, especially when the seeds x_0 and y_0 are equal. Notice that 5 is a primitive root, too.).

3. The period length of the sequence of pseudorandom numbers generated by the linear congruential method with $x_0 = 0$ and $x_{n+1} \equiv 4x_n + 7 \mod 25$ is 10 because $x_{10} \equiv 0$ and $x_i \not\equiv 0$ for $0 < i < 10$.

4. The linear congruential method $x_{n+1} \equiv x_n + c \mod m$ wouldn't be a good choice for generating pseudorandom numbers because -especially when n is large- after certain couple of steps one could observe that the increment in x_n is constant, so one could guess the next number x_{n+1} easily. If n is small, it is also bad, since the period is going to be small.

5. Pollard ρ-method with $x_0 = 2$ and $x_{n+1} = x_n^2 + 1$ gives $x_1 = 5$ and $x_2 = 26$ so that $(x_2 - x_1, N) = (21, 133) = 7$ (by euclidian algorithm). At the second step the other factor (13) falls out.

6. $x_{n+1} = ax_n + b$ would be a bad choice for x_n on the Pollard ρ-method. The main reason is that the sequence of numbers x_n wouldn't be randomly generated in the following sense: if $a > 1$, $x_{2n} - x_n = a(x_{2n-1} - x_{n-1})$, so all these differences are multiples of a. On the other hand, if $a = 1$, then $x_{2n} - x_n = x_0 + nb$; however, if m happens to share a common factor d with b, and if $x_0 \neq 0$ is not divisible by d, then Pollard ρ-method (with this choice of x_n's) will not tell us whether d is indeed a divisor of m. That explains why it is a bad choice.

7. We will show that composite Fermat numbers $2^{2^n} + 1$ are pseudoprimes to the base 2. Indeed, we have $2^{2^n} \equiv 1 \mod 2^{2^n} + 1$. Raise both sides of the congruence to the power $2^{2^n - n}$. We get $2^{2^{2^n}} \equiv 1 \mod 2^{2^n} + 1$, as required.

8. To show that 1387 is a pseudoprime to the base 2, one needs to check $2^{1387} \equiv 2 \mod 1387$. Observe that $1387 = 19 \cdot 73$, $1386 = 2 \cdot 3^2 \cdot 7 \cdot 11$. By Fermat, $2^{18} \equiv 1 \mod 19$. Hence $2^{18 \cdot 77} = 2^{1386} \equiv 1 \mod 19$. On the other hand, a simple calculation shows that $2^{18} \equiv 1 \mod 73$, and consequently $2^{1386} \equiv 2^{19 \cdot 72 + 18} \equiv 2^{18} \equiv 1 \mod 73$. Since $(19, 73) = 1$, these two congruences imply that $2^{1386} \equiv 1 \mod 1387$, which implies that $2^{1387} \equiv 2 \mod 1387$, as required. 1387, however, is not a strong pseudoprime to the base 2 because it does not pass Miller's test: $2^{1386/2} = 2^{693} \equiv 512 \not\equiv \pm 1 \mod 1387$. Indeed, $2^{693} \equiv 2^{18 \cdot 38} 2^9 \equiv 2^9 \equiv 512 \mod 1387$. Notice that we've used $2^{18} \equiv 1 \mod 1387$, which can be checked to be valid by hand. Finally, 1387 is not a Carmichael number because (a) $1387 = 19 \cdot 73$ is a product of distinct primes **but** (b) $72 = 73 - 1$ does NOT divide $1386 = 1387 - 1$.

9. To prove that 1373653 is a strong pseudoprime to the base 2, it suffices to show that $2^{(1373653-1)/2} = 2^{686826} \equiv -1 \mod 1373653$. To show this, note that $1373653 = 829 \cdot 1657$. Since 2 is a quadratic residue mod 1657 (because 1657 is 1 mod 8), say $a^2 \equiv 2 \mod 1657$, we have $2^{828} = a^{2 \cdot 828} = a^{1656} \equiv 1 \mod 1657$ by FlT. Again by Fermat we have $2^{828} \equiv 1 \mod 829$. Combining these using Chinese remainder theorem, we get $2^{828} \equiv 1 \mod 1373653$. So, $2^{686826} = 2^{828 \cdot 829} 2^{414} \equiv 2^{414} \mod 1373653$. Since $414 = 828/2$ and $2^{828} \equiv 1 \mod 1373653$, $2^{414} \equiv \pm 1 \mod 1373653$. We have $414 = 2 \cdot 3^2 \cdot 23$. Using a scientific calculator, it is possible to see that $2^{23 \cdot 2} \equiv -1 \mod 1373653$. So taking 9th power of both sides gives $2^{414} \equiv -1 \mod 1373653$, as required.