密 碼 學 與 應 用 作 業

94/11/10 (四)

1. (Trappe 2nd Ed. 3.13.3)
   (a) Find all solutions of $12x \equiv 28 \pmod{236}$
   (b) Find all solutions of $12x \equiv 30 \pmod{236}$

2. (Trappe 2nd Ed. 3.13.6)
   (a) Let $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ define the Fibonacci numbers 1,1,2,3,5,8,… Use the Euclidean algorithm to compute $\gcd(F_n, F_{n-1})$ for all $n \geq 1$
   (b) Find gcd(11111111, 11111)
   (c) Let a = 111…11 be formed with F_n repeated 1's and let b = 111…11 be formed with F_{n-1} repeated 1's. Find gcd(a, b). (Hint: Compare your computations in parts (a) and (b))

3. (Trappe 2nd Ed. 3.13.15)
   (a) Compute $\phi(d)$ for all of the divisors of 10 (namely, 1, 2, 5, 10), and find the sum of these $\phi(d)$.
   (b) Repeat part (a) for all of the divisors of 12
   (c) Let $n \geq 1$. Conjecture the value of $\Sigma\, \phi(d)$, where the sum is over the divisors of n. (This result is proved in many elementary number theory texts.)

4. (Trappe 2nd Ed. 3.13.19) Find all primes p for which $\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{p}$ is not invertible.

5. (Trappe 2nd Ed. 3.13.22)
   We want to find an exponent k such that $3^k \equiv 2 \pmod{65537}$
   (a) Observe that $2^{32} \equiv 1 \pmod{65537}$, but $2^{16} \not\equiv 1 \pmod{65537}$. It can be shown (Exercise 32) that 3 is a primitive root mod 65537, which implies that $3^n \equiv 1 \pmod{65537}$ if and only if $65536 \mid n$. Use this to show that $2048 \mid k$ but 4096 does not divide k. (Hint: Raise both sides of $3^k \equiv 2 \pmod{65537}$ to the 16-th and to the 32-nd powers.)
   (b) Use the result of part (a) to conclude that there are only 16 possible choices for k that need to be considered. Use this information to determine k. This problem shows that if p-1 has a special structure, for example, a power

of 2, then this can be used to avoid exhaustive searches. Therefore, such primes are cryptographically weak. See Exercise 9 in Chapter 7 for reinterpretation of the present problem.

6. (Trappe 2nd Ed. 3.13.29)

   Use the Legendre symbol to determine which of the following congruences have solutions (each modulus is prime)

   (a) $X^2 \equiv 123 \pmod{401}$

   (b) $X^2 \equiv 43 \pmod{179}$

   (c) $X^2 \equiv 1093 \pmod{65537}$

7. (Trappe 2nd Ed. 3.13.40)

   (a) Give an example of integers $m \neq n$ with $\gcd(m,n) > 1$ and integers a, b such that the simultaneous congruences

   $$x \equiv a \pmod{m}$$
   $$x \equiv b \pmod{n}$$

   have no solution.

   (b) Give an example of integers $m \neq n$ with $\gcd(m,n) > 1$ and integers $a \neq b$ such that the simultaneous congruences

   $$x \equiv a \pmod{m}$$
   $$x \equiv b \pmod{n}$$

   have a solution