Sample Exam#4 - with solutions

1. List all positive integers less than 30 that are relatively prime to 20.

2. Find $gcd(2^{89}, 2^{346})$ by directly finding the largest divisor of both numbers.

3. Find $lcm(2^{89}, 2^{346})$ by directly finding the smallest positive multiple of both numbers.

4. Find four integers b (two negative and two positive) such that $7 \equiv b \mod 4$.

5. Find the integer a such that $a = 71 \mod 47$ and $-46 \leq a \leq 0$.

6. (a) Convert $(11101)_2$ to base 10.

   (b) Convert $(2AC)_{16}$ to base 10.

   (c) Convert $(8091)_{10}$ to base 2.

   (d) Convert $(101011)_2$ to base 8.

7. Use the Euclidean algorithm to find $gcd(44, 52)$.
8. Use the Euclidean algorithm to find $gcd(300, 700)$.
9. Given that $gcd(620, 140) = 20$, write 20 as a linear combination of 620 and 140.

10. Find an inverse of 17 modulo 19.
11. (a) Solve the linear congruence $5x \equiv 3 \mod 11$
    (b) Solve the linear congruence $15x \equiv 31 \mod 47$ given that the inverse of 15 modulo 47 is 22.

    (c) Solve the linear congruence $31x \equiv 57 \mod 61$.

12. Show that 7 is a primitive root of 13.

13. Find the discrete logarithms of 5 and 8 to the base 7 modulo 13.

14. Use the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 2 \mod 3$, $x \equiv 1 \mod 4$, and $x \equiv 3 \mod 5$.

15. Find the sequence of pseudorandom numbers generated by the power generator $x_{n+1} = x_n^2 \mod 17$, and seed $x_0 = 5$.

16. A message has been encrypted using the function $f(x) = (x + 5) \mod 26$. If the message in coded form is JCFHY, decode the message.

17. Encrypt the message BALL using the RSA system with $n = 37 \cdot 73$ and $e = 7$, translating each letter into integers ($A = 00$, $B = 01, \ldots$) and grouping together pairs of integers.

18. What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667 1947 0671? (To decrypt, first find the decryption exponent $d$which is the inverse of $e = 13$ modulo $42 \cdot 58$.)