Sample Exam#4 - with solutions

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

   1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29.

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

   2^{89}

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

   2^{346}

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

   $3, 7, 11, 15, \ldots - 1, -5, -9, \ldots$

5. Find the integer a such that $a = 71 \mod 47$ and $-46 \leq a \leq 0$.
   -23

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

   29

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

   684

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

   1 1111 1001 1011

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

   $(53)_8$

7. Use the Euclidean algorithm to find $gcd(44, 52)$.
   4

8. Use the Euclidean algorithm to find $gcd(300, 700)$.
   100

9. Given that $gcd(620, 140) = 20$, write 20 as a linear combination of 620 and 140.

   $620 \cdot (-2) + 140 \cdot 9$

10. Find an inverse of 17 modulo 19.

    9

11. (a) Solve the linear congruence $5x \equiv 3 \mod 11$

        $5 + 11k$

    (b) Solve the linear congruence $15x \equiv 31 \mod 47$ given that the inverse of 15 modulo 47 is 22.

        24

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

        53

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

    The powers of 7 modulo 13 are $7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1$

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

    3, 9

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 $x \equiv 3 \mod 5$.

    Since 3, 4, and 5 are pairwise relatively prime, we can use the Chinese remainder theorem. The answer will be unique modulo $3 \cdot 4 \cdot 5 = 60$. Using the notation in the text,we have $a_1 = 2$, $m_1 = 3$, $a_2 = 1$, $m_2 = 4$, $a_3 = 3$, $m_3 = 5$, $m = 60$, $M_1 = 60/3 = 20$, $M_2 = 60/4 = 15$, $M_3 = 60/5 = 12$. Then we need to find inverses y_i of M_i modulo m_i for $i = 1, 2, 3$. This can be done by inspection (trial and error), since the moduli here are so small, or systematically using the Euclidean algorithm; we find that $y_1 = 2$, $y_2 = 3$, and $y_3 = 3$. Thus our solution is $x = 2{\cdot}20{\cdot}2+1{\cdot}15{\cdot}3+3{\cdot}12{\cdot}3 = 233 \equiv 53 \mod 60$. So the solutions are all integers of the form $53 + 60k$, where k is an integer.

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

    $8, 13, 16, 1, 1, 1, \ldots$

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.

    EXACT

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.

    1506 0075

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 $42 \cdot 58$.)

    SILVER