Week 01, problems.

Divisibility, GCD, Extended Euclidean algorithm, Congruences (introduction).

1. Prove or give counter examples for the following statements:
   a) If $c|a$ and $c|b$ then $c|ab$
   b) If $c|a$ and $c|b$ then $c^2|ab$
   c) If $c \nmid a$ and $c \nmid b$ then $c \nmid ab$
   d) For a prime p, if $p \nmid a$ and $p \nmid b$ then $p \nmid ab$

2. What is $gcd(6m + 5, 7m + 6)$, where m is an integer?

3. Evaluate $gcd(57, 209)$ and then use the Extended Euclidean algorithm to express the gcd as a linear combination of these numbers.

4. a) How many positive divisors does 8800 have?
   b) How many common positive divisors do 8800 and 99000 have?

5. Determine whether the following statements are true or not:
   a) $81 \equiv 43 \pmod{19}$, b) $4567890 \equiv -135790 \pmod{100}$,
   c) $21^{1000} \equiv 0 \pmod{7^{100}}$, d) $81 \cdot 10^{23} \equiv 43 \cdot 10^{23} \pmod{19}$

---

6. Show that for any integer a, 3 divides $a^3 - a$.

7. What is $gcd(k, k - 2)$, where k is an integer?

8. Evaluate $gcd(465, 2205)$ and then use the Extended Euclidean algorithm to express the gcd as a linear combination of these numbers.

9. How many integers are there between 1 and 1000 which have an equal number of even and odd divisors?

10. For the integer x, the congruence $x \equiv 7 \pmod{555}$ holds. Determine whether the following statements are true or not (in all possible cases):
    a) $x + 10 \equiv 17 \pmod{555}$, b) $3x \equiv 21 \pmod{555}$,
    c) $3x \equiv 21 \pmod{1665}$, d) $x^2 \equiv 49 \pmod{555}$,
    e) $2^x \equiv 2^7 \pmod{555}$, f) $x^{100} \equiv 7^{100} \pmod{555}$.

11. Show that if $2^n - 1$ is prime for an integer $n \geq 1$, then n is also a prime. (In other words $M(n)$ can be a Mersenne prime only when n is a prime)

---

12. Show that for every integer n, there exist n consecutive natural numbers that are composite.

13. What is $(2n^2 - 1, n + 1)$, where n is an integer?

14. Show that $n! + 1$ and $(n + 1)! + 1$ are relatively prime.

15. Evaluate $gcd(1066, 42)$ and then use the Extended Euclidean algorithm to express the gcd as a linear combination of these numbers.

16. Determine whether the following statements are true or not:
    a) $22^{23} + 24 \equiv 25 \pmod{11^{12}}$, b) $64 \cdot 2025^{2025} \equiv 157 \cdot 2025^{2025} \pmod{31}$,

17. For which positive integers m do the following statements hold?
    a) $m + 13 \equiv m + 18 \pmod{m}$, b) $7m + 9 \equiv m^2 + 9 \pmod{m}$,
    c) $13 \equiv 613 \pmod{m}$ and $23 \equiv 617 \pmod{m}$, d) $7m + 61 \equiv 4m + 76 \pmod{m}$.

18. Determine all the prime numbers p for which $p + 10$ and $p + 14$ are also prime.

19. Show that if $2^n + 1$ is prime for an integer $n \geq 1$, then n is a power of 2. (In other words, $F(n)$ can be a Fermat prime only if $n = 2^m$ for some m).

20. A Persian shah has 100 wives, and there are also 100 prisoners languishing in his prison, in cells numbered from 1 to 100. There are circular locks on the prison cells such that with one rotation a locked cell becomes open and an open cell becomes locked. On the shah's birthday, the 100 wives march through the prison and play with the locks. The first wife turns every lock once, the second wife turns every second door lock once, and so on, with the k^{th} wife turning every k^{th} door lock once, all the way to the 100^{th} wife. Finally, the prisoners whose doors are open are freed. What are the numbers of the cells where the lucky ones live?
b) On the shah's next birthday, the wives play with the locks again. Now the first wife turns every lock once, the second wife turns every second door lock twice, etc., the k^{th} wife turns every k^{th} door lock k times, all the way up to the 100^{th} wife. Now what are the numbers of the cells whose prisoners are freed? (Assume that by the next birthday, there are again prisoners in all the 100 cells.)

Final Answers

1. yes, yes, no, yes
2. 1
3. $19, 209 \cdot (-1) + 57 \cdot 4$
4. 36, 24
5. yes, no, yes, yes
6. Decompose it, 3 divides one of the factors.
7. 1 if k is odd, otherwise 2
8. $15, 465 \cdot 19 - 2205 \cdot 4$
9. 250
10. yes, yes, yes, yes, no, yes
11. Proof by contradiction
12. (Hint: Consider divisibility of $n! + i$)
13. 1
14. gcd is $\leq n$, but it is also $> n$
15. $2, 1066 \cdot 8 - 42 \cdot 203$
16. no, yes
17. a) 1,5, b) all positive integers, c) 1,2,3,6, d) 1,3,5,15
18. p can only be 3
19. Show that for any odd m, $2^m + 1$ is not a prime.
20. square numbers, numbers of the form $m \cdot 2^k$ where m is an odd square