

Feb. 4, 1997

1. If m is square free and $kj \equiv 1 \pmod{\phi(m)}$, show that $a^{kj} \equiv a \pmod{m}$ for all integers a , and why this is important for *coding theory*?
2. Find all primitive solutions in positive integers of the equation $x^2 + 7y^2 = z^2$ if y is even.
3. If p is an odd prime and $(abc, p) = 1$, show that the number of solutions (x, y) modulo p of the equation $ax^2 + by^2 \equiv c \pmod{p}$ is $p - \left(\frac{-ab}{p}\right)$.

Hint: $\sum_{y=1}^p \left(\frac{y^2 + k}{p}\right) = -1$ if $(k, p) = 1$.

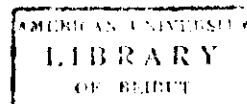
4. Find the number of integers n , $1 \leq n \leq p$ such that $\left(\frac{n}{p}\right) = \left(\frac{n+2}{p}\right) = -1$

5. If p is a prime, $p \equiv 1 \pmod{4}$, and $p = a^2 + b^2$ with a odd and positive, show that $\left(\frac{a}{p}\right) = 1$. (Hint: Use the reciprocity law of the Jacobi symbol)

6. Use the Chinese Remainder theorem to show that $x^2 \equiv a \pmod{p_1 p_2 \dots p_k}$ is solvable if $x^2 \equiv a \pmod{p_i}$ is solvable for each i . (p_1, p_2, \dots, p_k are distinct primes)

7. Compute $\left(\frac{5}{13}\right)$ by Gauss Lemmas 1 and 2.

8. Find all integer solutions of $10x + 14y + 35z = 1$.



9. Show that there are infinitely many primes of the form $8k+1$.

Hint: Every prime divisor of $x^4 + 1$ is of the form $8k+1$. (prove it!)

10. Let p and q be odd primes such that $q = 2p+1$ and $p \equiv 1 \pmod{4}$. Show that 2 is a primitive root modulo q .

Hint: Find $\left(\frac{2}{q}\right)$ from $p=4k+1$. Then apply Euler's Criterion.

11. Let p be an odd prime and $(a, p) = 1$. Show that $x^n \equiv a \pmod{p^m}$ is solvable if

$$a^{\frac{\phi(p^m)}{d}} \equiv 1 \pmod{p^m} \text{ where } d = \text{g.c. } d(n, \phi(p^m))$$

Hint: Let g be a primitive root modulo p^m , $x = g^t$ and $a = g^b$. Then solve for t .

12. Show that the number e is irrational.

Hint: $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!} + \dots$ If $e = \frac{i}{k}$, multiply both sides (of the above equation) by $k!$. Then discover the rest of the proof.

13. Prove the reciprocity law of the Legendre symbol using *Gauss sums* knowing the fact concerning G^2 .

