PRIME NUMBERS

Consider the set of all even integers $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$. We can add, subtract, and multiply elements of $2\mathbb{Z}$, and the result will always be in $2\mathbb{Z}$, but we cannot always divide. We can define divisibility and factorization in $2\mathbb{Z}$ in a similar way to that in $\mathbb{Z}$. (For example, $2|4$ in $2\mathbb{Z}$, but $2 \nmid 6$ even though $6 = 2 \cdot 3$, because $3 \notin 2\mathbb{Z}$.) A prime in $2\mathbb{Z}$ is a positive even integer that cannot be factored into the product of two even integers.

(a) Find all the primes in $2\mathbb{Z}$.

(b) Can every positive element of $2\mathbb{Z}$ be expressed as a product of these primes?

(c) If this factorization into primes can be accomplished, is it unique?

CONGRUENCES

7. Show that an integer of the form $5n + 3$, where $n \in \mathbb{P}$, can never be a perfect square.

Solve the following equations in the given set of integers modulo m.

46. $[3][x] = [18]$ in $\mathbb{Z}_{19}$

47. $([x] - [2])([x] - [3]) = [0]$ in $\mathbb{Z}_6$

57. If p is an odd prime, show that $x^2 \equiv a \pmod{p}$ has a solution for exactly half the values of a between 1 and $p - 1$ inclusive. Furthermore, if $1 \leq a \leq p - 1$ and $x^2 \equiv a \pmod{p}$ has a solution, show that it has exactly two congruence classes of solutions modulo p.

58. Does $x^3 \equiv a \pmod{p}$ always have a solution for every value of a, whenever p is prime?

61. Prove that $n^{91} \equiv n^7 \pmod{91}$ for all integers n. Is $n^{91} \equiv n \pmod{91}$ for all integers n?

62. For which positive values of k is $n^k \equiv n \pmod{6}$ for all integers n?

63. For which positive values of k is $n^k \equiv n \pmod{4}$ for all integers n?

95. (a) Prove that if p and q are relatively prime and x is an integer such that

$$\begin{aligned} x &\equiv p \pmod{q} \\ x &\equiv q \pmod{p}, \end{aligned}$$

then $x \equiv p + q \pmod{pq}$.

(b) Show by means of a counterexample that the condition that p and q are relatively prime is necessary.

CRYPTOGRAPHY

Encrypt each message M, using the RSA public key (e, n).

$$M = 2425, \quad (e, n) = (17, 28459)$$

Decrypt each received ciphertext C, using the RSA private key (d, n).

$$C = 32, \quad (d, n) = (77, 119)$$