

4. Prove that a decimal integer is divisible by 3 if and only if the sum of its digits is divisible by 3, and that it is divisible by 9 if and only if the sum of its digits is divisible by 9.
5. Prove that $n^5 - n$ is always divisible by 30.
6. Suppose that in tiling a floor that is 8 ft \times 9 ft, you bought 72 tiles at a price you cannot remember. Your receipt gives the total cost before taxes as some amount under \$100, but the first and last digits are illegible. It reads \$?0.6?. How much did the tiles cost?
7. (a) Suppose that m is either a power p^α of a prime $p > 2$ or else twice an odd prime power. Prove that, if $x^2 \equiv 1 \pmod{m}$, then either $x \equiv 1 \pmod{m}$ or $x \equiv -1 \pmod{m}$.
 (b) Prove that part (a) is always false if m is not of the form p^α or $2p^\alpha$, and $m \neq 4$.
 (c) Prove that if m is an odd number which is divisible by r different primes, then the congruence $x^2 \equiv 1 \pmod{m}$ has 2^r different solutions between 0 and m .
8. Prove “Wilson’s Theorem,” which states that for any prime p : $(p-1)! \equiv -1 \pmod{p}$. Prove that $(n-1)!$ is *not* congruent to $-1 \pmod{n}$ if n is *not* prime.
9. Find a 3-digit (decimal) number which leaves a remainder of 4 when divided by 7, 9, or 11.
10. Find the smallest positive integer which leaves a remainder of 1 when divided by 11, a remainder of 2 when divided by 12, and a remainder of 3 when divided by 13.
11. Find the smallest nonnegative solution of each of the following systems of congruences:

$$\begin{array}{lll}
 \text{(a)} \quad x \equiv 2 \pmod{3} & \text{(b)} \quad x \equiv 12 \pmod{31} & \text{(c)} \quad 19x \equiv 103 \pmod{900} \\
 x \equiv 3 \pmod{5} & x \equiv 87 \pmod{127} & 10x \equiv 511 \pmod{841} \\
 x \equiv 4 \pmod{11} & x \equiv 91 \pmod{255} & \\
 x \equiv 5 \pmod{16} & &
 \end{array}$$

12. Suppose that a 3-digit (decimal) positive integer which leaves a remainder of 7 when divided by 9 or 10 and 3 when divided by 11 goes evenly into a six-digit natural number which leaves a remainder of 8 when divided by 9, 7 when divided by 10, and 1 when divided by 11. Find the quotient.
13. In the situation of Proposition I.3.3, suppose that $0 \leq a_j < m_j < B$ for all j , where B is some large bound on the size of the moduli. Suppose that r is also large. Find an estimate for the number of bit operations required to solve the system. Your time estimate should be a function of B and r , and should allow for the possibility that r is either very large or very small compared to the number of bits in B .
14. Use the repeated squaring method to find $38^{75} \pmod{103}$.