MATH 114

Test 2 - Solutions

November 5, 2004

1. (a) Find an inverse of 5 modulo 8.

   $8 = 1 \cdot 5 + 3$
   $5 = 1 \cdot 3 + 2$
   $3 = 1 \cdot 2 + 1$
   $1 = 3 - 2 = 3 - (5 - 3) = 3 - 5 + 3 = 2 \cdot 3 - 5 = 2(8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5$
   Therefore -3 is an inverse of 5 modulo 8.

   (b) Solve the congruence $5x \equiv 7(\text{mod } 8)$.

   Multiply both sides of the congruence by -3:
   $-15x \equiv -21(mod\ 8)$
   $x \equiv -21(mod\ 8)$
   $x \equiv 3(mod\ 8)$

2. Solve the system

$$\begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 2(\text{mod } 7) \\ x \equiv 1(\text{mod } 10) \end{cases}$$

   $M = 3 \cdot 7 \cdot 10 = 210$, $M_1 = 70$, $M_2 = 30$, $M_3 = 21$.
   Next we find y_1, y_2, y_3 s.t. $70y_1 \equiv 1(mod\ 3)$, $30y_2 \equiv 1(mod\ 7)$, and $21y_3 \equiv 1(mod\ 10)$.
   Rewrite $70y_1 \equiv 1(mod\ 3)$ as $y_1 \equiv 1(mod\ 3)$, so we can take $y_1 = 1$.
   Rewrite $30y_2 \equiv 1(mod\ 7)$ as $2y_2 \equiv 1(mod\ 7)$, so we can take $y_2 = 4$.
   Rewrite $21y_3 \equiv 1(mod\ 10)$ as $y_3 \equiv 1(mod\ 10)$, so we can take $y_3 = 1$.
   Then $x \equiv 70 \cdot 1 \cdot 0 + 30 \cdot 4 \cdot 2 + 21 \cdot 1 \cdot 1 = 240 + 21 = 261(mod\ 210)$ or $x \equiv 51(mod\ 210)$.

3. Prove that for any nonnegative integer n, $n^3 + 5n$ is divisible by 6.

   There are many different proofs. Here is one. $n^3 + 5n = n^3 - n + 6n = (n - 1)n(n + 1) + 6n$. $(n - 1)n(n + 1)$ is the product of 3 consecutive numbers, so at least one of them is even and at least one of them is divisible by 3. Therefore the product is divisible by both 2 and 3 and so is divisible by 6. Clearly $6n$ is divisible by 6. Thus $(n - 1)n(n + 1) + 6n$ is divisible by 6.

4. Use Mathematical Induction to prove that for any positive integer n,

$$1 \cdot 2 + 2 \cdot 3 + \ldots + n(n + 1) = \frac{1}{3}n(n + 1)(n + 2).$$

   Basis step: $n = 1$. The formula gives $1 \cdot 2 = \frac{1}{3} \cdot 1 \cdot 2 \cdot 3$ which is true.
   Inductive step: Assume the formula holds for $n = k$, i.e.
   $1 \cdot 2 + 2 \cdot 3 + \ldots + k(k + 1) = \frac{1}{3}k(k + 1)(k + 2)$.
   We want to show that the formula holds for $n = k + 1$.
   $1 \cdot 2 + 2 \cdot 3 + \ldots + k(k + 1) + (k + 1)(k + 2) = \frac{1}{3}k(k + 1)(k + 2) + (k + 1)(k + 2) = \left(\frac{1}{3}k + 1\right)(k + 1)(k + 2) = \frac{k+3}{3}(k + 1)(k + 2) = \frac{1}{3}(k + 1)(k + 2)(k + 3)$.

5. A password must contain 8 characters. Each character can be either a digit or a letter. The password must contain at least one digit and at least one letter. How many different passwords are possible?

   Since there are 10 digits and 26 letters, there are 36^8 strings of lenght 8. But 26^8 strings consist entirely of letters (so they do not contain any digits) and 10^8 strings consist entirely of digits (so they do not contain any letters). Therefore there are $36^8 - 10^8 - 26^8$ possible passwords.