

Solutions 8

#1 Solve $7x = 3 \pmod{1001}$.

Since 7 is prime and does not divide 1003 (check!), there is $7^{-1} \pmod{1003}$. Use the Euclidean Algorithm to find it: $1003 - 143 \cdot 7 = 2$, $7 - 3 \cdot 2 = 1$. Then, going backward,

$$1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (1003 - 143 \cdot 7) = 430 \cdot 7 - 3 \cdot 1003$$

Looking at this mod 1003, we see that $7^{-1} = 430 \pmod{1003}$. Then the solution is

$$x = 7^{-1} \cdot 3 = 430 \cdot 3 = 1290 = 287 \pmod{1003}$$

#2 Solve

$$\begin{cases} 3x = 7 \pmod{101} \\ 5x = 11 \pmod{103} \end{cases}$$

First, we need to re-express each congruence in the simpler form " $x = a \pmod{m}$ ": either by intuition or via the Euclidean Algorithm, $3^{-1} = 34 \pmod{101}$ and $5^{-1} = 62$. Thus, the system is equivalent to

$$\begin{cases} x = 3^{-1} \cdot 7 = 34 \cdot 7 = 238 = 36 \pmod{101} \\ x = 5^{-1} \cdot 11 = 62 \cdot 11 = 686 = 64 \pmod{103} \end{cases}$$

Now run Euclid on 101 and 103. It's short: $103 - 1 \cdot 101 = 2$, $101 - 50 \cdot 2 = 1$, so running backward gives

$$1 = 101 - 50 \cdot 2 = 101 - 50 \cdot (103 - 101) = 51 \cdot 101 - 50 \cdot 103$$

Thus, by the usual trick, the system of congruences is equivalent to the single congruence

$$x = 51 \cdot 101 \cdot 64 - 50 \cdot 103 \cdot 36 = 9025 \pmod{101 \cdot 103}$$

#3 For ideals I, J in a commutative ring R with identity 1, prove that $I + J$ is an ideal.

We must prove that $I + J$ with addition is a subgroup of R -with-addition, and that it is closed under multiplication by elements of R . First, $0 = 0 + 0 \in I + J$, so 0 is in it. Second, for $x \in I$ and $y \in J$, $-x \in I$ and $-y \in J$ since I and J themselves are additive subgroups. Thus, $-(x + y) = (-x) + (-y) \in I + J$, and we have closure under inverses. For $x, x' \in I$ and $y, y' \in J$,

$$(x + y) + (x' + y') = (x + x') + (y + y') \in I + J$$

since I and J are themselves closed under addition. Thus, $I + J$ is an additive subgroup. Now let $x \in I$ and $y \in J$, and $r \in R$. Then

$$r(x + y) = rx + ry \in rI + rJ \subset I + J$$

since I and J are themselves ideals. Thus, $I + J$ is an ideal in R .