M328K Homework 5

Joshua Dong

February 21, 2014

0.1 3.7.8

$18x + 33y = 549$ where $x, y > 0$ and $x, y \in \mathbb{Z}$
Find: $\min(x + y)$

We first find $x, y > 0$ such that $18x + 33y = (18, 33) = 3$
By inspection, $18(2) + 33(-1) = 3$ is a solution to the above equation.
$549 = 183(3)$
$= 183(18(2) + 33(-1))$
$= (183)18(2) + (183)33(-1)$
$= 18(366) + 33(-183)$.
$\therefore \forall n \in \mathbb{Z}, 549 = 18(366 - 33(n)) + 33(-183 + 18(n))$.
$\therefore\ 549 = 18(3) + 33(15)$ when $n = 11$
$n > 11 \rightarrow x < 0$ and $n < 11 \rightarrow y < 0$.
$\therefore\ n = 11, x = 3, y = 15$.
$\therefore \min(x + y) = 3 + 15 = 18$.

0.2 4.1.26

Show that if $a^k \equiv b^k \pmod{m}$ and $a^{k+1} \equiv b^{k+1} \pmod{m}$ where $a, b, k, m \in \mathbb{Z}$ with $k, m > 0$ such that $(a, m) = 1$, then $a \equiv b \pmod{m}$. Is $(a, m) = 1$ required to show this?

$a^{k+1} \equiv\ b^{k+1} \pmod{m}$
$a \cdot\ a^k \equiv\ b \cdot\ b^k \pmod{m}$
$a \cdot\ a^k \equiv\ b \cdot\ a^k \pmod{m}$.
$a^k \perp\ m \leftrightarrow a \nmid m$ by the fundamental theorem of arithmetic.
$(a, m) = 1$.
$\therefore a \nmid m$
$\therefore\ a^k \perp\ m$
$a^k \perp\ m \rightarrow\ a \equiv\ b \pmod{m}$ by modular division by numbers coprime to the modulus.
If $(a, m) \neq 1$ then modular division would be prohibited and the result could not be shown.

0.3 4.1.30

Show $4^n \equiv 1 + 3n \pmod 9 \quad \forall n \in \mathbb{Z}^+$ using induction.

Base case:
If $n = 1$, then $4^1 \equiv 1 + 3(1) \pmod 9 \because 4 \equiv 4 \pmod 9$
Inductive Step:
Suppose the conclusion is valid for $n = k$.
That is, suppose we have $4^n \equiv 1 + 3n \pmod 9$.
$\therefore\ 4(4^n) \equiv\ 4(1 + 3n) \pmod 9$
$\therefore 4^{n+1} \equiv\ 4 + 12n \pmod 9$
$\therefore\ 4^{n+1} \equiv\ 4 + 3n \pmod 9 \because\ 9n \equiv\ 0 \pmod 9\ \forall\ n \in\ \mathbb{Z}^+$
$\therefore 4^{n+1} \equiv\ 1 + 3(n + 1) \pmod 9$, so the conclusion holding for $n = k$ implies that it hold for $n = k + 1$, and $4^n \equiv\ 1 + 3n \pmod 9 \quad \forall\ n \in\ \mathbb{Z}^+$.

0.4 4.1.34

Show that if $p \in\ \mathbf{P}$ and $k \in \mathbb{Z}^+$, the solutions to $x^2 \equiv\ x \pmod{p^k}$ can be represented as the set $\{x \in \mathbb{Z}^+ \mid\ x \equiv\ 0 \pmod{p^k} \text{ or } x \equiv\ 1 \pmod{p^k}\}$.

$p^k \mid\ (x^2 - x)$ by the definition of modulus.
$\therefore\ p^k \mid\ x(x - 1)$.
$\therefore$ either $p^k \mid\ x$ or $p^k \mid\ (x - 1)$ because $x \perp\ (x - 1) \quad \forall\ x \in\ \mathbb{Z}$.
Case $p^k \mid\ x$:
$p^k \mid\ (x - 0)$
$\therefore\ x \equiv\ 0 \pmod{p^k}$.
Case $p^k \mid\ (x - 1)$:
$x \equiv\ 1 \pmod{p^k}$ by definition of modulo.
$\therefore$ either $x \equiv\ 0 \pmod{p^k}$ or $x \equiv\ 1 \pmod{p^k} \quad \forall\ p \in\ \mathbf{P},\ k \in \mathbb{Z}^+$