M328K Homework 6

Joshua Dong

March 8, 2014

2(e), 14(b,d), 16, 18

0.1 4.2.2.e

Find all solutions to $128x \equiv 833 \pmod{1001}$

$(128, 1001) = (128, 1001 - 8(128)) = (128, -23) = 1$
$\therefore$ there is exactly one unique solution mod 1001.
$128x - 1001q = 1$
$1001 + (-8)128 = -23$
$128 + (5)((1)1001 + (-8)128) = 13$
$(1)1001 + (-8)128 + (2)((1)128 + (5)((1)1001 + (-8)128)) = 3$
$(128+(5)((1)1001+(-8)128))+(-4)((1)1001+(-8)128+(2)((1)128+(5)((1)1001+(-8)128))) = 1$
$128+(5)1001+(-40)128+(-4)1001+(32)128+(-8)128+(-40)1001+(320)128 = 1$
$(-39)1001 + (305)128 = 1$
$\therefore 1\bar{2}8 = 305.$
$1\bar{2}8(128x) \equiv 1\bar{2}8(833) \pmod{1001}.$
$\therefore x \equiv 305(833) \equiv 812 \pmod{1001}$
$\therefore x \in S$ where $S = \{n \mid n = 812 + 1001k \;\; \forall k \in \mathbb{Z}\}$.

0.2 4.2.14.b

$2x + 4y \equiv 6 \pmod 8$

$x + 2y \equiv 3 \pmod 4$
$(1, 2, 4) \mid 3$
$4n = (x + 2y - 3)$ for some $n \in \mathbb{Z}$.
$(x + 2y - 4n) = 3.$
Let k be some integer where $2k = (2y - 4n)$.
Then $(x + 2k) = 3.$
By observation, we see that one solution is $x = 3$, $k = 0$.
All solutions to the previous equation then are expressible in the form:
$x = 3 - 2t, k = t \;\; \forall t \in \mathbb{Z}.$

Now we solve $2k = (2y - 4n)$.
$k = (y - 2n)$.
First we solve $y - 2n = 1$
By observation, we see that one solution is:
$y = 3, n = 1$
So the solution to $k = (y - 2n)$ is:
$y = 3k + 2s, n = k - s \ \ \forall s \in \mathbb{Z}$.
$\therefore x = 3 - 2t, y = 3t + 2s \ \ \forall s, t \in \mathbb{Z}$ represent all the solutions to $x + 2y \equiv 3 \pmod 4$.

0.3 4.2.14.d

$10x + 5y \equiv 9 \pmod{15}$

$(10, 5, 15) \nmid 9$
Thus, there are no solutions.

0.4 4.2.16

Show $x^2 \equiv 1 \pmod{2^k}$ has exactly four unique solutions: $\pm 1, \pm(1 + 2^{k-1})$ when $k > 2$. Also show the cases for $k \equiv 1, k \equiv 2$.

If $k = 1$*:*
$x^2 \equiv 1 \pmod 2$
$\therefore 2 \mid (x^2 - 1)$
$\therefore 2 \mid (x + 1)(x - 1)$.
If x is even, then the product $(x + 1)(x - 1)$ is odd and not divisible by 2.
If x is odd, then the product $(x + 1)(x - 1)$ is even and divisible by 2.
$\therefore$ x must be odd.
The set of odd numbers congruent mod 2 less than 2 is $\{1\}$.
$\therefore x \in S$ where $S = \{n \mid n \equiv 1\}$.
$\therefore$ There is one unique solution if $k = 1$.

If $k = 2$*:*
$x^2 \equiv 1 \pmod 4$
$\therefore 4 \mid (x^2 - 1)$
$\therefore 4 \mid (x + 1)(x - 1)$.
If x is even, then the product $(x + 1)(x - 1)$ is odd and not divisible by 4.
If x is odd, then $(x + 1)$ is even and $(x - 1)$ is even.
The product of two numbers divisible by 2 is divisible by 4.
$\therefore$ If x is odd, then 4 divides the product $(x + 1)(x - 1)$.
$\therefore$ x must be odd.
The set of odd numbers congruent mod 4 less than 4 is $\{1, 3\}$.
$\therefore x \in S$ where $S = \{n \mid n \equiv 1$ or $n \equiv 3\}$.
$\therefore$ There are two unique solutions if $k = 2$.

If $k > 2$*:*
$x^2 \equiv 1 \pmod{2^k}$
$\therefore 2^k \mid (x^2 - 1)$
$\therefore 2^k \mid (x + 1)(x - 1)$.
If x is even, then the product $(x + 1)(x - 1)$ is odd and not divisible by any power of 2 greater than 0.
If x is odd, then the product $(x + 1)(x - 1)$ is even and divisible by 2.
$\therefore$ any solutions that exist must be even.
Let n be an integer where $2n + 1 = x$.
Then $2^k \mid ((2n + 1) + 1)((2n + 1) - 1)$.
$\therefore 2^k \mid (2n + 2)(2n)$
$\therefore 2^k \mid (4)(n)(n + 1)$.
Since $k > 2$,
$2^{k-2} \mid (n)(n + 1)$.
$m2^{k-2} = (n)(n + 1)$ for some integer m.
If $m = 0$*, then:*
$n = 0$ or $n + 1 = 0$.
$\therefore n \in \{-1, 0\}$ provides all solutions where $m = 0$.
$\therefore x \in \{-1, 1\}$ provides all solutions where $m = 0$.
If $m \neq 0$*, then:*
If n is even, then n+1 is odd.
If n is odd, then n+1 is even.
$2^{k-2} \mid (n)(n + 1)$.
$\therefore$ either $2^{k-2} \mid n$ or $2^{k-2} \mid (n + 1)$.
$\therefore x \in S$ where $S = \{n \text{ such that } 2^{k-2} \mid n \text{ or } 2^{k-2} \mid (n + 1) \ \ \forall k \in \mathbb{Z}, k > 2\}$ provides all solutions where $m \neq 0$.
$\therefore n \in S$ where $S = \{n \text{ such that } n = t2^{k-2} \text{ or } n = t2^{k-2} - 1 \ \ \forall k, t \in \mathbb{Z}, k > 2\}$ provides all solutions where $m \neq 0$.
$\therefore x \in S$ where $S = \{x \text{ such that } x = t2^{k-1} + 1 \text{ or } x = t2^{k-1} - 1 \ \ \forall t, k \in \mathbb{Z}, k > 2\}$ provides all solutions where $m \neq 0$.
$\therefore x \in S$ where $S = \{x \text{ such that } x \equiv 2^{k-1} + 1 \pmod{2^k} \text{ or } x \equiv 2^{k-1} - 1 \pmod{2^k} \ \ \forall k \in \mathbb{Z}, k > 2\}$ provides all solutions where $m \neq 0$.
$\therefore$ In the general case where $m \in \mathbb{Z}$, $x \in S$ where $S = \{x \text{ such that } x = -1 \text{ or } x = 1 \text{ or } x \equiv 2^{k-1} + 1 \pmod{2^k} \text{ or } x \equiv 2^{k-1} - 1 \pmod{2^k} \ \ \forall k \in \mathbb{Z}, k > 2\}$ provides all solutions where $m \neq 0$.

0.5 4.2.18

$p \in \mathbf{P}, p > 2, a \in \mathbb{Z}^+, a \perp p \to x^2 \equiv a \pmod{p}$ has 0 or 2 unique solutions.

Since $a \equiv 1 \pmod{p}$,
$p \mid (a - 1)$
$p \mid (x^2 - 1)$
$p \mid (x + 1)(x - 1)$.
$\therefore x + 1$ or $x - 1$ must divide p.
$p \mid (x + 1) \to p \nmid (x - 1)$ and $p \mid (x - 1) \to p \nmid (x + 1)$
$\therefore$ there are two unique solutions $\mod p$: $x \equiv p - 1$ and $x \equiv 1$.