Assignment 4

Egregious error in Devoir 3 solutions: alternative solution to 2(b). We wrote:
"Then $a(x-y) \equiv 0 \bmod m$. We are assuming $x \not\equiv y \bmod m$, so $a \equiv 0 \bmod m$, contradicting $(a,m) = 1$."
Of course, $ab \equiv 0 \bmod m$ does not necessarily imply that $a \equiv 0$ or $b \equiv 0 \bmod m$, though this is true if m is prime. For example $2 \cdot 3 \equiv 0 \bmod 6$. We should have written the following:
If $E' \subsetneq E$, there exists $x, y \in E$ with $x \not\equiv y \bmod m$ such that $ax + b \equiv ay + b \bmod m$, that is $ax \equiv ay \bmod m$. Now $(a,m) = 1$ so $aa' \equiv 1 \bmod m$ for some a'. Then $aa'x \equiv aa'y \bmod m$, that is $x \equiv y \bmod m$, a contradiction.

5. *(1 point.)* Any integer $n \equiv \pm\ell \bmod 10$ for some $\ell \in \{1,2,3,4,5\}$, so $n^2 \equiv \ell^2 \bmod 10$, and $\ell^2 = 0, 1, 4, 5, 6$ or $9 \bmod 10$.

6. *(1 point.)* We claim that $4^n \equiv 4$ or $6 \bmod 10$ $(n > 0)$. This is true for $n = 1, 2$. Suppose it's true for $n = 1, 2, \ldots, k$. Then $4^{k+1} = 4 \cdot 4^k \equiv 4 \cdot 4 \equiv 6$ or $4 \cdot 6 \equiv 4 \bmod 10$. Our claim follows by induction.

7. *(1 point.)* $(n+1)^3 - n^3 = n^3 + 3n^2 + 3n + 1 - n^3 = 3(n^2 + n) + 1 \equiv 1 \bmod 3$.

9. *(1 point.)* $3^6 \equiv (3^2)^3 \equiv 2^3 \equiv 1 \bmod 7$, $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\} \equiv \{1, 2, 3, 4, 5, 6\} \bmod 7$.

10. *(1 point.)* If $m = 2k + 1$, the sum is $0 + 1 + m - 1 + 2 + m - 2 + \cdots + k + m - k \equiv km \equiv 0 \bmod m$.

11. *(2 points.)* If $(r,m) = 1$ then $(m - r, m) = 1$, for if $p \mid m, m - r$ then $p \mid r$. If $r = m - r$ then $(m, r) = r = 1$ implies $m = 2$. Therefore a reduced system of residues modulo $m > 2$ has the form $\{r_1, m - r_1, r_2, m - r_2, \ldots, r_n, m - r_n\}$, and the sum over this set is congruent to $r_1 + (m - r_1) + \cdots r_n + (m - r_n) \equiv nm \equiv 0 \bmod m$.

12. *(2 points.)* Obviously $\{r \bmod p : (r,p) = 1\} = \{1 \bmod p, 2 \bmod p, \ldots, p - 1 \bmod p\}$, so by Wilson's Theorem,

$$r_1 r_2 \cdots r_{p-1} \equiv 1 \cdot 2 \cdots (p-1) \equiv -1 \bmod p.$$

13. *(1 point.)* $m = 6, a = 1, b = 1, E = \{1, 5\}, E' = \{2, 6\}$.

15. *(3 points.)* By inspection, (a) $x \equiv 4 \bmod 7$, (b) $x \equiv 6 \bmod 9$, that is $x \equiv 6$ or $15 \bmod 18$, (f) $x \equiv 3 \bmod 8$, (c) has no solution since $12x \equiv 0 \not\equiv 9 \bmod 6$, (h) has no solution since $20x \equiv 0 \not\equiv 30 \bmod 4$, (g) has no solution for otherwise we have integers x, y such that $20x = 30y + 4$, that is $10(2x - 3y) = 4$, but 4 is not a multiple of 10. In general $ax \equiv b \bmod m$ if and only if $ax - my = b$ for integers x, y if and only if (a,m) divides b (the solutions is unique modulo m if $b = (a,m)$), and we use the Euclidean algorithm to find x, y.

(d) $x \equiv 47 \bmod 52$.

$$\begin{aligned}
52 &= 23 \cdot 2 + 6 \\
23 &= 6 \cdot 3 + 5 \\
6 &= 5 \cdot 1 + 1 \\
1 &= 6 - 5 \\
&= 6 - (23 - 6 \cdot 3) \\
&= 6 \cdot 4 - 23 \\
&= (52 - 23 \cdot 2) \cdot 4 - 23 \\
&= 52 \cdot 4 - 23 \cdot 9 \\
41 &= 52 \cdot (4 \cdot 41) - 23 \cdot 9 \cdot 41 \\
41 &\equiv 23 \cdot 9 \cdot (-41) \equiv 23 \cdot 9 \cdot 11 \equiv 23 \cdot 99 \equiv 23 \cdot 47 \bmod 52.
\end{aligned}$$

(e) $x \equiv 5, 35, 65,$ or $95 \bmod 120$. $68x \equiv 100 \bmod 120$ if and only if $17x \equiv 25 \bmod 30$ if and only if $x \equiv 5 \bmod 30$.

$$\begin{aligned}
30 &= 17 + 13 \\
17 &= 13 + 4 \\
13 &= 4 \cdot 3 + 1 \\
1 &= 13 - 4 \cdot 3 \\
&= 13 - (17 - 13) \cdot 3 \\
&= 13 \cdot 4 - 17 \cdot 3 \\
&= (30 - 17) \cdot 4 - 17 \cdot 3 \\
&= 30 \cdot 4 - 17 \cdot 7 \\
25 &= 30 \cdot 4 \cdot 25 - 17 \cdot 7 \cdot 25 \\
25 &\equiv 17 \cdot 7 \cdot (-25) \equiv 17 \cdot 7 \cdot 5 \equiv 17 \cdot 5 \bmod 30.
\end{aligned}$$

Supplementary question. *(4 points.)* For each $r \in \{1, \dots, m\}$, let r_* be the unique integer in $\{1, \dots, m\}$ such that $rr_* \equiv 1 \bmod m$. (Thus $r_{**} = r$, of course $r = r_*$ is possible.) Then

$$1 \equiv \prod_{\substack{1 \le r \le m \\ (r,m)=1}} rr_* \equiv \prod_{\substack{1 \le r \le m \\ (r,m)=1}} r^2 \bmod m.$$

Bonus question. We claim that

$$\prod_{\substack{1 \le r \le m \\ (r,m)=1}} r \equiv \begin{cases} -1 \bmod m & \text{if } m = 4, p^\nu \text{ or } 2p^\nu \\ 1 \bmod m & \text{otherwise.} \end{cases}$$

The case $m = 2$ is trivial. Assume $m > 2$. Now

$$\prod_{\substack{1 \le r \le m \\ (r,m)=1}} r \equiv \prod_{\substack{1 \le r \le m \\ (r,m)=1 \\ r \ne r_*}} r \prod_{\substack{1 \le r \le m \\ (r,m)=1 \\ r = r_*}} r \equiv \prod_{\substack{1 \le r \le m \\ (r,m)=1 \\ r^2 \equiv 1 \bmod m}} r \bmod m.$$

First consider the cases $m = 4, p^\nu, 2p^\nu$ for some odd prime p. If $x^2 \equiv 1 \bmod 4$ then $x \equiv \pm 1 \bmod 4$. If $p > 2$ and $(x-1)(x+1) \equiv x^2 - 1 \equiv 0 \bmod p^\nu$ then p divides $x+1$ or $x-1$, but not both (for otherwise p divides $(x+1)-(x-1) = 2$), so $x = p^\nu + 1$ or $p^\nu - 1$. These are also the only solutions to $x^2 \equiv 1 \bmod 2p^\nu$, for in this case we must have $x^2 \equiv 1 \bmod 2$ and $x^2 \equiv 1 \bmod p^\nu$. Therefore the product is $1(-1) \equiv -1 \bmod m$ in these cases. For all other m we can prove our claim in two ways.

Alternative 1. Choose any $a \not\equiv 1 \bmod m$ such that $a^2 \equiv 1 \bmod m$. Then $\{r \bmod m : r^2 \equiv 1 \bmod m\} = \{ar \bmod m : r^2 \equiv 1 \bmod m\}$. To see this, note that $(ar) \equiv a^2 r^2 \equiv 1 \bmod m$ if $r^2 \equiv 1 \bmod m$, and $ar_1 \equiv ar_2 \bmod m$ if and only if $r_1 \equiv a^2 r_1 \equiv a^2 r_2 \equiv r_2 \bmod m$. In fact $\{r \bmod m : r^2 \equiv 1 \bmod m\}$ has the form

$$\{r_1 \bmod m, ar_1 \bmod m, r_2 \bmod m, ar_2 \bmod m, \dots, r_N \bmod m, ar_N \bmod m\},$$

for $ar_i \equiv r_j \bmod m$ if and only if $r_i \equiv a^2 r_i \equiv ar_j \bmod m$, and $ar_i \equiv r_i \bmod m$ if and only if $a \equiv ar_i^2 \equiv r_i^2 \equiv 1 \bmod m$, but $a \not\equiv 1 \bmod m$. Then

$$\prod_{\substack{1 \le r \le m \\ (r,m)=1 \\ r^2 \equiv 1 \bmod m}} r \equiv r_1 ar_1 \cdot r_2 ar_2 \cdots r_N ar_N \equiv ar_1^2 \cdot ar_2^2 \cdots a_N r_N^2 \equiv a^N \bmod m.$$

Similarly, if $b \not\equiv a, 1 \bmod m$ and $b^2 \equiv 1 \bmod m$, then this product is congruent to $b^N \bmod m$. Now if $N = 2n+1$ is odd, then $a^N \equiv a(a^2)^n \equiv a \bmod m$, and likewise $b^N \equiv b \bmod m$, so $a \equiv a^N \equiv b^N \equiv b \bmod m$, a contradiction. Hence N is even, and $a^N \equiv b^N \equiv 1 \bmod m$.

We have proved that the product is $1 \bmod m$ if there are at least three distinct solutions modulo m to $x^2 \equiv 1 \bmod m$ ($\pm 1 \bmod m$ and $a \not\equiv \pm 1 \bmod m$). Indeed, if $m \neq 1, 2, 4, p^\nu, 2p^\nu$, then $m = \alpha\beta$ for some coprime $\alpha, \beta > 2$. Let u, w be integers such that $\alpha u - \beta w = -2$, and let $a = \alpha u + 1 = \beta w - 1$. Then $a^2 = uwm - (\alpha u - \beta w) - 1 = uwm + 2 - 1 \equiv 1 \bmod m$. Suppose $a \equiv \pm 1 \bmod m$. Then $a \equiv \pm 1 \bmod \alpha, \beta$, so either $\alpha u \equiv 0 \bmod \beta$, hence $-2 = \alpha u - \beta w \equiv 0 \bmod \beta$, or $\beta w \equiv 0 \bmod \alpha$, hence $2 = \beta w - \alpha u \equiv 0 \bmod \alpha$. Then α or β divides 2, a contradiction. Hence $a \not\equiv \pm 1 \bmod m$. Our claim is proved.

Alternative 2. If r is a solution to $x^2 \equiv 1 \bmod m$, then so is $-r$, and $r \not\equiv -r \bmod m$ ($m > 2$). If $\pm r_1 \bmod m, \pm r_2 \bmod m, \ldots, \pm r_N \bmod m$ are all of the distinct solutions modulo m to the congruence $x^2 \equiv 1 \bmod m$, then the product is congruent to

$$r_1(-r_1)\cdots r_N(-r_N) \equiv (-1)^N \bmod m,$$

where $2N$ is the number of distinct solutions to the congruence $x^2 \equiv 1 \bmod m$. We will prove that N is even, and our claim follows. In the cases $m \neq 1, 2, 4, p^\nu, 2p^\nu$, we have given three distinct solutions $\pm 1 \bmod m, a \bmod m$ to $x^2 \equiv 1 \bmod m$. Of course $-a \bmod m$ is another solution, so in fact we have at least four.

Suppose $x_1 \bmod m, \ldots, x_n \bmod m$ are solutions such that

$$x_{i_1} \cdots x_{i_k} \equiv x_{j_1} \cdots x_{j_\ell} \bmod m$$

if and only if $\{i_1, \ldots, i_k\} = \{j_1, \ldots, j_\ell\}$ ($\subseteq \{1, \ldots, n\}$). Let

$$S_n = \left\{ \prod_{i \in I} x_i \bmod m : I \subseteq \{1, \ldots, n\} \right\}$$

(define the product over $I = \emptyset$ to be 1). Suppose $y \bmod m \notin S_n$ and $y^2 \equiv 1 \bmod m$. If $y x_{i_1} \cdots x_{i_k} \equiv x_{j_1} \cdots x_{j_\ell} \bmod m$ for some $\{i_1, \ldots, i_k\}, \{j_1, \ldots, j_\ell\} \subseteq \{1, \ldots, n\}$, then $y \equiv y(x_{i_1} \cdots x_{i_k})^2 \equiv x_{i_1} \cdots x_{i_k} x_{j_1} \cdots x_{j_\ell} \bmod m$, that is $y \bmod m \in S_n$, a contradiction. If $y x_{i_1} \cdots x_{i_k} \equiv y x_{j_1} \cdots x_{j_\ell} \bmod m$, then multiplying by y we get $x_{i_1} \cdots x_{i_k} \equiv x_{j_1} \cdots x_{j_\ell} \bmod m$, a contradiction. Hence

$$S_{2n} = \left\{ \prod_{i \in I} x_i \bmod m, y \prod_{i \in I} x_i \bmod m : I \subseteq \{1, \ldots, n\} \right\}$$

is a set of distinct solutions to $x^2 \equiv 1 \bmod m$. We have our set $S_4 = \{\pm 1, \pm a\}$ of four distinct solutions, and the set of all solutions is S_{2n} for some n. Now $\#S_{2n} = 2^s \#S_4 = 2^{s+2}$ for some s. Hence N is even.

Alternative 3. We can actually determine the exact number of solutions modulo m to $x^2 \equiv 1 \bmod m$ with less work. Write $m = 2^{\nu_0} p_1^{\nu_1} \cdots p_t^{\nu_t}$, where $\nu_0 \geq 2$ or $t \geq 2$. We will prove that the number of solutions is 2^t if $\nu_0 = 0$ or 1, 2^{t+1} if $\nu_0 = 2$, and 2^{t+2} if $\nu_0 > 2$.

Consider the case $\nu_0 = 0, t \geq 2$. Choose integers u_i, w_i such that $u_i p_i^{\nu_i} + w_i m / p_i^{\nu_i} = 1$, $i = 1, \ldots, t$. Note that $w_i m / p_i^{\nu_i} \equiv 1 \bmod p_i^{\nu_i}$ and $w_i m / p_i^{\nu_i} \equiv 0 \bmod p_j^{\nu_j}$ if $i \neq j$. Thus if

$$y = \sum_{i=1}^{t} (-1)^{n_i} w_i m / p_i^{\nu_i}, \quad (n_i = 1 \text{ or } 2)$$

then $y^2 \equiv (-1)^{2n_i} \equiv 1 \bmod p_i^{\nu_i}$ for each i, therefore $y^2 \equiv 1 \bmod m$ by the Chinese Remainder Theorem. If

$$y' = \sum_{i=1}^{t} (-1)^{n_i'} w_i m / p_i^{\nu_i}, \quad (n_i' = 1 \text{ or } 2)$$

and $y' \equiv y \bmod m$, then $y' \equiv y \bmod p_i^{\nu_i}$ for each i, so $(-1)^{n_i'} = (-1)^{n_i}$ for each i. Therefore the 2^t combinations $\pm w_1 m/p_1^{\nu_1} \pm \cdots \pm w_t m/p_t^{\nu_t}$ are all distinct modulo m. Finally, there are no other solutions modulo m, for if $z^2 \equiv 1 \bmod m$ then $z^2 \equiv \pm 1 \bmod p_i^{\nu_i}$ for each i, so $z \equiv y \bmod m$ for one of the solutions y we have already determined.

The other cases are similar. In the case $\nu_0 = 1$, there are the same number of solutions because there is only one solution modulo 2 to $y^2 \equiv 1 \bmod 2$. In the case $\nu_0 = 2$, we have twice as many solutions because $y^2 \equiv 1 \bmod 2^2$ obviously has two solutions modulo 2^2. In the case $\nu_0 > 2$, we have four times as many solutions, because there are precisely four solutions modulo 2^{ν_0} to $y^2 \equiv 1 \bmod 2^{\nu_0}$. For if $(y+1)(y-1) \equiv 0 \bmod 2^{\nu_0}$, then evidently 2 divides both $y+1$ and $y-1$, but 2^2 cannot divide both $y+1$ and $y-1$, for otherwise it divides the difference 2. It follows that $y \equiv \pm 1, \pm(1 + 2^{\nu_0 - 1}) \bmod 2^{\nu_0}$ are the only solutions, and they are clearly distinct modulo 2^{ν_0}.

17 points, plus 3 points for a reasonable attempt at all questions = 20 points.