Test 2

Sam Grayson

April 26, 2015

1. Write a complete residue system mod 17 only using multiples of 3.

   $0 \equiv 3 \cdot 0 \pmod{17}$
   $1 \equiv 3 \cdot 6 \pmod{17}$
   $2 \equiv 3 \cdot 12 \pmod{17}$
   $3 \equiv 3 \cdot 18 \pmod{17}$
   $4 \equiv 3 \cdot 24 \pmod{17}$
   $5 \equiv 3 \cdot 30 \pmod{17}$
   $6 \equiv 3 \cdot 36 \pmod{17}$
   $7 \equiv 3 \cdot 42 \pmod{17}$
   $8 \equiv 3 \cdot 48 \pmod{17}$
   $9 \equiv 3 \cdot 54 \pmod{17}$
   $10 \equiv 3 \cdot 60 \pmod{17}$
   $11 \equiv 3 \cdot 66 \pmod{17}$
   $12 \equiv 3 \cdot 72 \pmod{17}$
   $13 \equiv 3 \cdot 78 \pmod{17}$
   $14 \equiv 3 \cdot 84 \pmod{17}$
   $15 \equiv 3 \cdot 90 \pmod{17}$
   $16 \equiv 3 \cdot 96 \pmod{17}$

   $\{0, 18, 36, 54, 72, 90, 108, 126, 144, 162, 180, 198, 216, 234, 252, 270, 288\}$ forms a complete residue system mod 17. I generated the table above using the following Python code. For an explanation of Python code in general and the source for `linear_diophantine()`, please read 3.23 in my notebook.

```
from tools import linear_diophantine
CRS = []
for n in range(17):
    (x_0, y_0), (r_x, r_y) = linear_diophantine(3, -17, n)
    # now we have 3x_0 - 17y_0 = n
    # output n ≡ 3 · x_0 (mod 17)
    print (r'${n} \equiv 3 \cdot {x_0} \pmod{{17}}$ \\'.format(**locals()))
    CRS.append(3 * x_0)

# output the whole CRS, seperated by commas
print (', '.join(map(str, CRS)))
```

2. Find $2^{100} \pmod 9$.

   All congruence statements are taken mod 9.

$$\begin{aligned} 2^{100} &\equiv \ ? \\ &\equiv 2^{3\cdot 33+1} \\ &\equiv (2^3)^{33}\cdot 2^1 \\ &\equiv 8^{33}\cdot 2 \\ &\equiv (-1)^{33}\cdot 2 \\ &\equiv -1\cdot 2 \\ &\equiv 7 \end{aligned}$$

3. **Theorem:** For any CRS mod m, multiplying by a natural coefficient coprime to m produces a new CRS.

   Let $\{r_1, r_2, \ldots, r_m\}$ form a CRS mod m. Let $a \in \ mathbbN$ where $\gcd(a, m) = 1$.

   Proof: Theorem 3.17 states that m unique (unique mod m) elements describe a CRS. Begin with $\{r_1, r_2, \ldots, r_m\}$ which is a CRS, so the elements are unique by definition. $r_i \not\equiv r_j \rightarrow ar_i \not\equiv ar_j$ by the inverse of theorem 1.14 (The inverse is necessarily true since theorem 1.14 is an 'if-and-only-if'). Thus $\{ar_1, ar_2, \ldots, ar_m\}$ are all unique. To reiterate: If they were not $(ar_i \equiv ar_j)$ we could use theorem 1.14 to draw a contradiction $(r_i \equiv r_j)$ which is not true by the definition of the CRS. Therefore $\{ar_1, ar_2, \ldots, ar_m\}$ constitue m unique elements. By theorem 3.17 they must also constitute a CRS mod m.

4. Find the number x where $x \equiv 1 \pmod 4$ and $x \equiv 2 \pmod 3$.

   $$\begin{aligned} &x \equiv 1 \pmod 4 && \{\ldots, 1, 5, 9, 13, 17, 21, 25, 29, \ldots\} \\ &x \equiv 2 \pmod 3 && \{\ldots, 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, \ldots\} \\ &\left.\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 2 \pmod 3 \end{aligned}\right\} && \{\ldots, 5, 17, 29, \ldots\} \end{aligned}$$

   The first solutions set is $\{1, 5, 9, \ldots\}$. By exhaustion, 5 is the first number in the solution set of the first congruence that also satisfies the second congruence. The LCM of the two modulos is 12. Therefore $x \equiv 5 \pmod{12}$.

5. **Theorem**: Let the digits of n be $n = a_k a_{k-1} \ldots a_0$. Let $m = a_0 - a_1 + a_2 \cdots \pm a_{k-1} \mp a_k$. 11 divides n exactly when 11 divides m.

   All congruences are taken mod 11.

   Proof: Let $f_n(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$. We know that $-1 \equiv 10$, which implies $f(-1) \equiv f(10)$ by theorem 3.8. However, $f(-1) = a_k \pm a_{k-1} \mp \cdots + a_0 = m$. Similarly $f(10) = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_0 = n$. Therefore by substitution $m \equiv n$. If $11 \mid n$, then $n \equiv 0 \pmod{11}$, then $m \equiv 0$ by 1.11 (transitivity), which gives $11 \mid m$. And vice versa, If $11 \mid m$, then $m \equiv 0$, then $n \equiv 0$, then $11 \mid n$. Therefore $11 \mid m \leftrightarrow 11 \mid n$. ∎

6. Create a test to see if $4|n$. Let the digits of $n = n_m \ldots n_1 n_0$.

   Algorithm: If n_1 is even, $4|n$ exactly when $4|n_0$. If n_1 is odd, $4|n$ exactly when $4|(n_0 + 2)$.

   Lemma: $n|(na + b) \leftrightarrow n|b$. Justification: $n|na$ by defintion of divides. $n|na$ and $n|(na + b)$ imply $n|(na + b - na)$ by Theorem 1.2. $n|b$ and $n|na$ imply $n|(na + b)$ by Theorem 1.1.

   Lemma: If a_0 is even or odd, then $a_m \ldots a_2 a_1 a_0$ is likewise. Justification: By the previous lemma $2|((a_m \ldots a_2 a_1) \cdot 10 + a_0)$ is equivalent to $2|a_0$ since $2|((a_m \ldots a_2 a_1) \cdot 10)$. Therefore if $2 \nmid a_0$, then $2 \nmid (a_m \ldots a_2 a_1 a_0)$ and vice versa if a_0 is even.

Proof (odd): If n_1 is even, then $n_m \dots n_2 n_1$. Then $4|(n_m \dots n_2 n_1 n_0)$ is equivalent to $4|(2k \cdot 10 + n_0)$, is equivalent to $4|(4k \cdot 5 + n_0)$, is equivalent to $4|n_0$ (reduced the problem to less than 8).

Proof (even): If n_1 is odd, then $n_m \dots n_2 n_1$ is odd. Then $4|(n_m \dots n_2 n_1 n_0)$ is equivalent to $4|(2k+1) \cdot 10 + n_0$, is equivalent to $4|(20k + 10 + n_0)$, is equivalent to $4|(10 + n_0)$, is equivalent to $4|(8 + 2 + n_0)$, is equivalent to $4|(2 + n_0)$ (reduced the problem to less than 11. ∎

7. The egg problem.

$x \equiv 1 \pmod 2$
$x = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23 \dots\}$
$x \equiv 2 \pmod 3$ and all previous equations
$x = \{5, \underline{11}, 17, \underline{23}, 29, 35, 41, \underline{47} \dots\}$
$x \equiv 3 \pmod 4$ and all previous equations
$x = \{\underline{11}, \underline{23}, \underline{35}, \underline{47}, 59, 71, 83, 95, 107, 119, 131, 143, 155, 167, 179, \dots\}$
$x \equiv 4 \pmod 5$ and all previous equations
$x = \{59, 119, 179, \dots\}$
$x \equiv 5 \pmod 6$ and all previous equations
$x = \{59, \overline{119}, 179, \dots\}$
$x \equiv 0 \pmod 7$ and all previous equations
$x = \{\overline{119}, 539, 959, 1379, 1799, 2219, \dots\}$

Therefore, there are at least 119 eggs in the basket.

8. **Theorem**: $\{2, 4, 6, \dots, 2m\}$ is a CRS mod m if m is odd.

Proof: Show that any element of the CCRS is congruent to exactly one thing in S where $S = \{2, 4, \dots, 2m\}$. For all x in the CCRS ($0 \leq x < m$),

- if x is even and non-zero, it is in the set S. $x \equiv x \wedge x \in s$. Moreover it is in the set uniquely, the next possible reperesentation is $x + m$, which is not in the set S because an even plus an odd is an odd and the set contains only evens.
- If x is zero, $x \equiv 2m \pmod m$ since $m|(2m - 0)$. $0 \equiv 2m \wedge 2m \in S$. (This is why I believe the question should ask about the set $\{0, 2, 4, \dots 2m - 2\}$, playful nudge). Moreover it is in the set uniquely because no other element is perfectly divisibly by m other than $2m$.
- If x is odd, $x = 2 \cdot \frac{x-1}{2} + 1$ and since m is odd, $m = 2 \cdot \frac{m-1}{2} + 1$. Then $x \equiv x + m$ since $m|(x+m-x)$ and $x+m$ is even, since an odd plus an odd is an even. $x < m-2$ since x is a smaller odd number than m, therefore $x+m < 2m-2 < 2m$. $x \equiv x+m \wedge x+m \in S$. Moreover it is in the set uniquely since the only other representation of x between 0 and $2m$ is x, and x is odd therefore it is not in the set S.

Since every element in the CCRS is congruent to exactly one number in S, and every integer is congruent to exactly one number in the CCRS, every integer is congruent to exactly one number in S. Therefore S is a CRS. ∎

All odd numbers can be written $2k + 1$ for some $k \in \mathbb{Z}$. All even numbers can be written $2k$ for some $k \in \mathbb{Z}$. An even number plus an even number is even since $2k_1 + 2k_2 = 2(k_1 + k_2)$.

An even number pulss an odd number is odd since $2k_1 + 2k_2 + 1 = 2(k_1 + k_2) + 1$. An odd number plus an odd number is even since $2k_1 + 1 + 2k_2 + 1 = 2(k_1 + k_2 + 1)$. In general, the sum of two addends is even exactly when both addends are even or both addends are odd. $2|(a + b) \leftrightarrow (2|a \leftrightarrow 2|b)$.

9. **Theorem:** All reduced residue systems modulo m have the same number of elements.

   Let $R = \{r_1, r_2, \ldots, r_i\}$ be a Reduced Residue System (RRS) modulo m with i elements, and similarly $S = \{s_1, s_2, \ldots, s_j\}$ with j elements. All congruence statements are taken mod m.

   Proof: Assume for contradiction that $i \neq j$ (without loss of generality $i < j$). By the first tenet of the definition of RRS, $\gcd(s_p, m) = 1$ for all p. By the third tenet of the definition, there exists a q where $s_p \equiv r_q$. Since there are more ss than rs, some of the ss have to be congruent to the same r (in other words the relation can not be injective). $s_p \equiv r_q \equiv s_t$ for some t. By transitivity $s_p \equiv s_t$. This contradicts tenet 2 of the definition.

   Therefore $i = j$. ∎

10. **Theorem**: $ax \equiv ay \pmod{n} \leftrightarrow a \equiv y \pmod{\frac{n}{\gcd(a,n)}}$

    Proof of $\rightarrow$ conditional: Let $ax \equiv ay \pmod{n}$. This is equivalent to $n|(ax - ay)$, which is equivalent to $n|a(x-y)$, which is equivalent to $\frac{n}{\gcd(a,n)} \gcd(a, n)|\frac{a}{\gcd(a,n)}(x-y)$. Since $\gcd(a, n)$ shows up in the divisor and the dividend, they cancel out. $\frac{n}{\gcd(a,n)}|\frac{a}{\gcd(a,n)}(x - y)$. By Test 1 Theorem 4, $\frac{n}{\gcd(a,n)}$ and $\frac{a}{\gcd(a,n)}$ are coprime, which fulfills the condition for Theorem 1.41, which claims that $\frac{n}{\gcd(a,n)}|(x - y)$, which is equivalent to $x \equiv y \pmod{\frac{n}{\gcd(a,n)}}$.

    $ab|ac$ exactly when $b|c$. If $b|c$ then $c = ib$, then $ac = iab$, then$ab|ac$. If $ab|ac$ then $iab = ac$, then $ib = c$, then $b|c$.

    Proof of $\leftarrow$ conditional: