Notebook Swag

Sam Grayson

April 20, 2015

3.1 $2^5 \equiv -9 \pmod{41}$ — $2^5 = 32 = 41 - 9$
$(2^5)^4 \equiv (-9)^4 \pmod{41}$ — By theorem 1.18
$2^{20} \equiv 81^2 \pmod{41}$ — $(2^5)^4 \equiv (-9)^4 \equiv ((-9)^2)^2 \pmod{41}$
$2^{20} \equiv (-1)^2 \pmod{41}$ — $(2^5)^4 \equiv (81)^2 \equiv (2 \cdot 41 - 1)^2 \pmod{41}$
$2^{20} - 1 \equiv 0$ — $2^{20} \equiv (-1)^2 \equiv 1$ and theorem 1.13

$41 \mid (2^{20} - 1 - 0)$ iff $41 \mid (2^{20})$ ■

3.2 $37^{453} \equiv 1^{453} \equiv 1 \pmod{12}$

3.3 $2^{50} \equiv (2^3)^{16} \cdot 2^2 \equiv 1^{16} \cdot 4 \equiv 4 \pmod{7}$

3.4
$$9^{453} \equiv (9^2)^{(453-1)/2} \cdot 9 \equiv 9^{226} \cdot 9 \pmod{12}$$
$$9^{226} \equiv (9^2)^{226/2} \equiv 9^{113} \pmod{12}$$
$$9^{113} \equiv (9^2)^{(113-1)/2} \cdot 9 \equiv 9^{56} \cdot 9 \pmod{12}$$
$$9^{56} \equiv (9^2)^{56/2} \equiv 9^{28} \pmod{12}$$
$$9^{28} \equiv (9^2)^{28/2} \equiv 9^{14} \pmod{12}$$
$$9^{14} \equiv (9^2)^{14/2} \equiv 9^{7} \pmod{12}$$
$$9^{7} \equiv (9^2)^{(7-1)/2} \cdot 9 \equiv 9^{3} \cdot 9 \pmod{12}$$
$$9^{3} \equiv (9^2)^{(3-1)/2} \cdot 9 \equiv 9^{1} \cdot 9 \pmod{12}$$
$$9 \cdot 9 \equiv 9 \pmod{12}$$

3.5
$$17^{48} \equiv (17^2)^{48/2} \equiv 16^{24} \pmod{39}$$
$$16^{24} \equiv (16^2)^{24/2} \equiv 22^{12} \pmod{39}$$
$$22^{12} \equiv (22^2)^{12/2} \equiv 16^{6} \pmod{39}$$
$$16^{6} \equiv (16^2)^{6/2} \equiv 22^{3} \pmod{39}$$
$$22^{3} \equiv (22^2)^{(3-1)/2} \cdot 22 \equiv 16^{1} \cdot 22 \pmod{39}$$
$$16 \cdot 22 \equiv 1 \pmod{39}$$

$$5^{24} \equiv (5^2)^{24/2} \equiv 25^{12} \pmod{39}$$
$$25^{12} \equiv (25^2)^{12/2} \equiv 1^{6} \pmod{39}$$
$$1^{6} \equiv 1 \pmod{39}$$

3.6 **Algorithm:**

1. Reduce a to its remainder mod r. Let $a = nq + t$ and $0 < t \leq n$ from the Division Algorithm. $nq = (a - t)$, therefore $n \mid (a - t)$ by definition of divides, therefore $a \equiv t \pmod{n}$ by definition of divides, therefore $a^r \equiv t^r \pmod{n}$ by theorem 1.18.

2. If $r = 1$, return a
3. Calculate a^2
4. If r is even, return the solution to $(a^2)^{r/2} \equiv k \pmod{n}$ (calculation can be done recursively with this same algorithm).
5. If r is odd, return ak where k is the solution to $(a^2)^{(r-1)/2} \equiv k \pmod{n}$.

This uses at most $2\log_2 j$ multiplications where n is upper-bounded like so $n < 2^j$.

3.7 **Exercise:** When $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, does $f(98) \equiv f(-100) \pmod{99}$?

Since $98 - (-100) = 198$ and $2 \cdot 99 = 198$, then $98 \equiv -100$. $98^i \equiv (-100)^i$ by theorem 1.18, and $a_i 98^i \equiv a_i(-100)^i$ by theorem 1.14, and finally $a_i 98^i + c \equiv a_i(-100)^i + c$ by thorem 1.12. For the first term c can be a_0 and i can be 1. For the ith term (assuming the polynomial is equal up to the $(i-1)$th term), c can be the previous part of the polynomial (truncated right before i). Therefore by induction $f(98) = f(-100)$.

3.8 **Theorem:** $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$

Proof: For all integer i, $a^i \equiv b^i$ by theorem 1.18, $a_i a^i \equiv a_i b^i$ by theorem 1.14, and $a_i a^i + c \equiv a_i b^i + c$ for all integer c by theorem 1.12. Starting with $a_1 a^i + a_0 \equiv a_i b^i + a_0$, we can build up the rest of the polynomial congruences through induction. Assuming the two polynomials are congruent up to $i-1$, then let $a_{i-1}a^{i-1} + \cdots + a_0$ be c in $a_i a^i + c \equiv a_i b^i + c$. This just stacked one more term on. Therefore by induction $a_n a^n + a_{n-1}a^{n-1} \cdots + a_0 \equiv a_n b^n + a_{n-1}b^{n-1} \ldots a_0$.■

In fact, for any operator $\bumpeq$ (read "bumpy equals"),

$a \bumpeq b \wedge b \bumpeq c \rightarrow a \bumpeq c$	Transitivity
$a \bumpeq b \wedge c \bumpeq d \rightarrow a + c \bumpeq b + d$	Equality over equal additions

is enough to garuntee that for any polynomial $a \bumpeq b \rightarrow f(a) \bumpeq f(b)$. Since multiplication is repeated addition $a \bumpeq b \rightarrow \underbrace{a + \cdots + a}_{n \text{ times}} \bumpeq \underbrace{b + \cdots + b}_{n \text{ times}}$, therefore $na \bumpeq nb$. Since exponentation is repeated multiplication, by similar logic, $a^i \bumpeq b^i$. Then using equality of equal additions to add the finishing tuch $a^i + c \bumpeq b^i + d$ where $c \bumpeq d$. The proof above holds for $\bumpeq$ this as well. Notice that I cannot say $a^i + c \bumpeq b^i + c$, because I don't even have reflexivity.

3.9 **Theorem:** Let n be a natural number. Let m be the sum of digits of n. $9 \mid n \leftrightarrow 9 \mid m$. Let the digits of n be $n = a_k 10^k + a_{k-1}10^{k-1} \ldots a_0 10^0$.

Let $f_a(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$. $10 \equiv 1 \pmod{9}$, therefore $f(10) \equiv f(1) \pmod{9}$, therefore $a_k 10^k + a_{k-1}10^{k-1} \ldots a_0 10^0 \equiv a_k 1^k + a_{k-1}1^{k-1} + \cdots + a_0 1 \pmod{9}$, therefore $m \equiv n \pmod{9}$. If $m \equiv 0 \pmod{9}$, then $n \equiv 0 \pmod{9}$ and vice versa. Therefore $m \mid 9$ exactly when $n \mid 9$ ■

3.10 Let n be a natural number. Let m be the sum of digits of n. $3 \mid n \leftrightarrow 3 \mid m$.

By the same reasoning above, three works too. ■ In fact any number n where $1 \equiv 10 \pmod{n}$

works. We did some of this in lesson one, but it was markedly more painful. This method is easier to apply, but it is less flexible.

For example, in $n = a_k a_{k-1} \dots a_2 a_1 a_0$ is divisible by 4 if and only if a_2 is even and $a_1 a_0$ is divisible by 4 or a_2 is odd and $(a_1 a_0) - 2$ is divisible by 4. This cannot be proved the same way 3.9 and 3.10 were. It has to be proved the way 1.21, 1.22, and 1.23 were.

3.11 **Theorem:** Let f be an n-degree polynomial such that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $a_n > 0$. $\exists k \in \mathbb{N}(\forall x > k(f(x) > 0))$.

Proof: $x > |a_{n-1}|$ is sufficient for $x^n > a_{n-1}x^{n-1}$. That is because multiplying both sides of the condition by x^{n-1} (valid operation since $x^{n-1} > 0$, since $x > 0$) gives $xx^{n-1} > a_{n-1}x^{n-1}$, equivalently $x^n > a_{n-1}x^{n-1}$. That simply arises from the initial condition. After this point, the nth term dominates the $(n-1)$th term.

If the first term dominates the zeroth term at some point k_1, and the second term dominates the first term at some point k_2, then at some point greater than k_1 and greater than k_2, the third term dominates the second term and the second term dominates the first term $(|a_2x^2| > |a_1x| > |a_0|)$. Therefore the third term dominates the first term $(|a_2x^2| > a_0)$.

Continuing in this way, there is some point k_n the nth term dominates the $(n-1)$th term. The $(n-1)$th term dominates the $(n-2)$th term after k_{n-1}. Therefore for $x > k$ where $k = \max(k_n, k_{n-1}, \dots, k_1)$, the nth term dominates. $a_n > 0$ by the premise. Therefore $|a_nx^n| > |a_{n-1}x^{n-1}| > \cdots > |a_0|$. Therefore $n|a_nx^n| > |a_{n-1}x^{n-1}| + \cdots + |a_0|$. Since n is a positive constant multiplier, we can absorb it into a_n. If it dominates the first term, and the first term is positive, then whether or not the later terms are positive or negative the polynomial will be positive. Therefore, after the point k_n the first term dominates every other term by more than a factor of n. $\exists k \in \mathbb{N}(\forall x > k(f(x) > 0))$ ■

3.12 **Theorem:** Let $f(x) = a_nx^na_{n-1}x^{n-1} + \cdots + a_0$. $\forall y \in \mathbb{N}(\exists k \in \mathbb{N}(x > k \rightarrow f(x) > y))$

Proof: Construct the polynomial $g(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 + y$. By the previous theorem $\exists k \in \mathbb{N}(x > k \rightarrow g(x) > 0)$ which is tantamount to saying $\exists k \in \mathbb{N}(x > k \rightarrow f(x) > y)$, since $f(x) + y = g(x)$. ■

3.13 **Theorem:** Any integer-coefficient polynomial produces composite numbers for an infinite number of inputs.

Let f be an n-degree polynomial such that $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $a_n > 0$.

Proof: Pick a composite number x_1. Find the number k where $\forall x \in \mathbb{N}(x > k \rightarrow f(x) > f(c))$ whose existence is garunteed by Theorem 3.12. Find a number x_2 where $x_2 > k$ and $x_1 \equiv x_2 \pmod{}$, $f(d) \equiv f(c) \pmod{n}$ by theorem 3.8, $f(d) > f(c)$ by theorem 3.12, therefore $f(d) \equiv f(c) \pmod{n}$.

3.14 **Theorem:** $\forall i \in \mathbb{Z}(\forall j \in \mathbb{N}(\exists! r \in \mathbb{N}(i \equiv r \pmod{j} \land 0 \leq r < j)))$

Proof:

Let $i \in \mathbb{N}$	
Let $j \in \mathbb{N}$	
If $i > 0$	
Conclude: $\exists! q, r \in \mathbb{N}(i = qj + r \wedge 0 \leq r < j)$	Division algorithm
Otherwise $i < 0$	
$\exists! p, r \in \mathbb{N}(-i = pj + t \wedge 0 \leq t < j)$	Division algorithm
$i = -pj - j + j - t$	Algebra
$i = -(p+1)j + j - t$	Algebra
$-j < -t \leq 0$	Property of inequalities
$0 < j - t \leq j$	Property of inequalities
If $j - t < j$	
Let $q = -(p+1)$ Let $r = j - t$	
$0 < r < j$	Property of inequalities
$0 \leq r < j$	Property of inequalities
Conclude: $\exists! q, r \in \mathbb{N}(i = qj + r \wedge 0 \leq r < j)$	
Otherwise $j - t \geq j$	
$j - t = j$	Property of inequalities
$t = 0$	Identity property
$i = pj$ Let $r = 0$	
Conclude: $\exists! q, r \in \mathbb{N}(i = qj + r \wedge 0 \leq r < j)$	
$\forall i \in \mathbb{N}(\forall j \in \mathbb{N}(\exists! r \in \mathbb{N}(i \equiv r \pmod{j} \wedge 0 \leq r < j)))$	Either way ■

3.15
1. $\{0, 1, 2, 3\}$
2. $\{-4, -3, -2, -1\}$
3. $\{0, 5, 10, 15\}$

Let $A \in \text{CRS}(n)$ stand for A is a possible Complete Residue System (CRS) for mod n.

Let $A \in \text{CCRS}(n)$ stand for A is the Canonical Complete Residue System (CCRS) for mod n.

3.16 **Theorem:** $B \in \text{CRS}(n) \rightarrow |B| = n$

Proof:

Let $A \in \text{CCRS}(n)$	
Let $B \in \text{CRS}(n)$	For conditional
Let $f : A \rightarrow B$ where $a \mapsto b$ if $a \equiv b \pmod{n}$	
$\forall a \in A(\exists! b \in B(x \equiv b \pmod{n}))$	Definition of CRS
$\forall a \in \text{cod}(f)(\exists! b \in \text{dom}(f)(f(a) = b))$	Substitution
Thus f is a bijective map	
$\|A\| = n$	By inspection
Thus $\|A\| = \|B\| = n$	Bijection
$B \in \text{CRS}(n) \rightarrow \|B\| = n$	Conditional proof ■

3.17 **Theorem:** $\neg\exists a \in S(\exists b \in S(a \equiv b \pmod{n} \land a \neq b)) \to S \in \text{CRS}(n)$

Let $\text{rem}(x \pmod{n})$ (read "remainder of x modulo n")denote the number in the Complete Canonical Residue System congruent to x mod n.

Lemma: $a = b \to a \equiv b \pmod{n}$ **Proof:**

$a - b = 0$	Algebra
$0n = 0$	Zero-property of multiplication
$n \mid (a - b)$	Definition of divides
$a \equiv b \pmod{n}$	Definition of modulo ■

Proof:

Assume $\neg\exists a \in S(\exists b \in S(a \equiv b \pmod{n} \land a \neq b))$	(for conditional)
Assume $\exists a \in S(\exists b \in S(\text{rem}(a \pmod{n}) = \text{rem}(b \pmod{n})))$	(for contradiction)
$a \equiv \text{rem}(a \pmod{n})$	Definition of remainder
$b \equiv \text{rem}(b \pmod{n})$	Definition of remainder
$a \equiv \text{rem}(a \pmod{n}) \equiv b$	Lemma and transitivity
$\exists a \in S(\exists b \in S(a \equiv b \pmod{n} \land a \neq b))$	Existential generalization
$\neg\exists a \in S(\exists b \in S(\text{rem}(a \pmod{n}) = \text{rem}(b \pmod{n})))$	Contradiction

■

3.18
1. $x \equiv 1 \pmod{3}$
2. $x \equiv 4 \pmod{5}$
3. No solution.
4. $x \equiv 14 + 71n \pmod{213}$ for $n \in \{0, 1, 2\}$

3.19 **Theorem:** $\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \exists x, y \in \mathbb{Z}(ax - ny = b)$

Proof:

$\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \exists x \in \mathbb{Z}(b \equiv ax \pmod{n})$	Theorem 1.10
$\exists x \in \mathbb{Z}(b \equiv ax \pmod{n}) \leftrightarrow \exists x \in \mathbb{Z}(n \mid (b - ax))$	Definition of modulo
$\exists x \in \mathbb{Z}(n \mid (b - ax)) \leftrightarrow \exists x, y \in \mathbb{Z}(ny = b - ax)$	Definition of divides
$\exists x, y \in \mathbb{Z}(ny = b - ax) \leftrightarrow \exists x, y \in \mathbb{Z}(ax + ny = b)$	Algebra
$\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \exists x, y \in \mathbb{Z}(ax - ny = b)$	Transitivity ■

3.20 **Theorem:** $\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \gcd(a, n) \mid b$

Proof:

$\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \exists x, y \in \mathbb{Z}(ax - ny = b)$	Theorem 3.19
$\exists x, y \in \mathbb{Z}(ax - ny = b) \leftrightarrow \gcd(a, n) \mid b$	1.48
$\exists x \in \mathbb{Z}(ax \equiv b \pmod{n}) \leftrightarrow \gcd(a, n) \mid b$	Transitivity ■

3.21 It has a solution.

3.22 $213 - 8 \cdot 24 = 21$
$24 - 1 \cdot 21 = 3$
$24 - 1 \cdot (213 - 8 \cdot 24) = 3$
$9 \cdot 24 - 213 = 3$
$41 \cdot (9 \cdot 24 - 213) = 41 \cdot 3 = 123$
$369 \cdot 24 - 41 \cdot 213 = 123$
$(369 + n \cdot 71) \cdot 24 - (41 + n \cdot 8) \cdot 213 = 123$
$213 \mid ((369 + n \cdot 71) \cdot 24 - 213)$
$x = 369 + n \cdot 71$

3.23 **Algorithm:** Find all solutions of $ax = b \pmod{n}$ for $0 \leq x < n$

I wrote this algorithm in Python so that it would be more precise. I spent a lot of time making it accessible to non-programmers. Please spend as much time trying to understand it as I spent trying to make it understandable

First, there are four things you must understand about Python code:

- Lines that begin with a # are comments for the reader. They are ignored by the computer. They show up in gray.
- Single equals-sign means assignment of the right-hand value to the left-hand variable. `x = 2` says "Make x equal to 2." Double equals-sign tests for equivalence. `x == 2` asks the question "Is x equal to 2?". Ordered-pairs (called n-tuples) are allowed in any assignment or equality tests.
- Any statement that ends in a colon is a control-flow statement. It controls when the statements immediately following it are executed. Those statements are indented to show that they are dependent on the control-flow statement. For example, in the following code, lines 2 and 3 run only if x is 2 (from line 1) otherwise lines 5 and 6 run. Line 7 is not indented, so it is not controlled by the if-else from line 1. Line 9 runs once for every element in the set `[1, 2, 3, 4, 5]`, where each iteration `a` takes on one value from that list.

```
1 if x == 2:
2     a = 3
3     b = 5
4 else:
5     a = 6
6     b = 10
7 c = 4
8 for a in [1, 2, 3, 4, 5]:
9     n = n + a
```

- A function is defined by a line beginning with "def", the name of the function, a temporary name given to the function parameters, and then a colon (this is a kind of control-flow statement). The function ends with a line that says 'return' and then a value. `def f(x):` and then a line that says `return 2 * x`. If later you see `f(10)`, it evaluates to 20.

```python
def linear_diophantine(a, b, c):
    # Returns (x_0, y_0), (r_x, r_y) where $ax + by = c$
    # when $x = x_0 + nr_x$ and $y = y_0 + nr_y$
    g = gcd(a, b)
    if c == g:
        for x in count():
            # Loop over this with x = {0, 1, 2, 3 ...}
            if mod(a * x, g, b):
                # execute this block iff $a \cdot x \equiv g \pmod{b}$
                y = (g - a*x) / b
                # at this point $ax + by = g$
                # therefore x and y are solutions
                # theorem 1.53 states solutions for x are spaced b / g apart
                # and solutions for y are spaced -a / g apart
                return (x, y), (b / g, -a / g)
    else:
        # solve a simpler diophantine equation first
        (u_0, v_0), (r_u, r_v) = linear_diophantine(a, b, g)
        # at this point $ua + vb = g$
        # multiplying both sides by $\frac{c}{g}$ gives
        # $u_0\frac{c}{g}a + v_0\frac{c}{g}b = g\frac{c}{g} = c$
        (x_0, y_0) = (u_0 * c / g, v_0 * c / g)
        # the spacing between solutions doesn't change
        (r_x, r_y) = (r_u, r_v)
        return(x_0, y_0), (r_x, r_y)

def linear_congruence(a, b, n):
    # Returns x_0, n where $ax \equiv b \pmod{n}$ when $x \equiv x_0 \pmod{n}$
    # this function relies on the linear_diophantine function,
    # because why reinvent the wheel?
    (x_0, y_0), (x_i, y_i) = linear_diophantine(a, -n, b)
    return x_0, x_i
```

This code relies on auxiliary functions. They are listed below.

```python
# this is a funciton from the standard library
# count() -> {0, 1, 2, 3, ...}
from itertools import count

def cmod(a, n):
    # Returns c such that $a \equiv c \pmod{n}$ and $0 \leq c < n$ WLOG $n > 0$
    # this c is the remainder in the division algorithm
    # and c is in the canonical complete residue system
    n = abs(n)
    if a > 0:
```

```
        while a >= n:
            a = a - n
        return a
    else:
        while a < 0:
            a = a + n
        return a

def divides(d, a):
    # Returns true if d|a
    # (equivalent to if the remainder upon division is zero, return true)
    return cmod(a, d) == 0

def mod(a, b, n):
    # Returns true if a ≡ b (mod n)
    # (equivalent to n|(b − a))
    return divides(n, b - a)

def gcd(a1, b1):
    # Returns the greatest common multiple
    # WLOG a > b > 0
    a = max(abs(a1), abs(b1))
    b = min(abs(a1), abs(b1))
    r = cmod(a, b)
    if r == 0:
        return b
    else:
        return gcd(b, r)
```

Theorem: There are $\frac{n}{\gcd(a,n)}$ solutions to the linear congruence.

Proof:

$0 \le x_0 < \frac{n}{\gcd(a,n)}$

$0 + (\gcd(a,n) - 1)\frac{n}{\gcd(a,n)} \le x_0 + (\gcd(a,n) - 1)\frac{n}{\gcd(a,n)} < \frac{n}{\gcd(a,n)} + (\gcd(a,n) - 1)\frac{n}{\gcd(a,n)}$

$0 + (\gcd(a,n) - 1)\frac{n}{\gcd(a,n)} \le x_0 + (\gcd(a,n) - 1)\frac{n}{\gcd(a,n)} < \frac{n}{\gcd(a,n)} + \gcd(a,n)\frac{n}{\gcd(a,n)} - \frac{n}{\gcd(a,n)}$

$(\gcd(a,n) - 1)\frac{n}{\gcd(a,n)} \le x_0 + (\gcd(a,n) - 1)\frac{n}{\gcd(a,n)} < \gcd(a,n)\frac{n}{\gcd(a,n)}$

For all $0 \le m \le \gcd(a,n) - 1$, there are solutions at $x_0 + m\frac{n}{\gcd(a,n)}$ in the CCRS

There are $\gcd(a,n)$ solutions ∎

3.24 3.20, 3.23a, and 3.23b taken together prove this theorem. The big idea is that a linear congruence is a special kind of linear diophantine equation.

3.25 **Exercise:** Solve for x in

$x \equiv 3 \pmod{17}$
$x \equiv 10 \pmod{16}$
$x \equiv 0 \pmod{15}$

x satisfies $x \equiv 3 \pmod{17}$ when $x = 3 + j \cdot 17$
$x = \{3, 20, 37, 54, 71, 88, 105, 122, 139, 156, 173, 190, 207, 224, 241, 258, 275, 292, 309, 326, 343, 360, 377, 394, \ldots\}$

x satisfies $x \equiv 10 \pmod{16}$ and all previous equations when $x = 122 + j \cdot 272$
$x = \{122, 394, 666, 938, 1210, 1482, 1754, 2026, 2298, 2570, 2842, 3114, 3386, 3658, 3930, 4202, 4474, 4746, 5018, 5290, 5562, 5834, 6106, 6378, 6650, 6922, 7194, 7466, 7738, 8010, 8282, 8554, 8826, 9098, 9370, 9642, 9914, 10186, 10458, 10730, 11002, 11274, 11546, 11818, 12090, \ldots\}$

x satisfies $x \equiv 0 \pmod{15}$ and all previous equations when $x = 3930 + j \cdot 4080$
$x = \{3930, 8010, 12090, \ldots\}$

Notice that the next solution-set is all of the previous solutions that satisfy the next equation. The solution-set at each step is a subset of the solution-set above it. I have marked which numbers are 'carried over' from the previous solution-set to the next solution-set with color, underlines, and overlines.

3.26 **Exercise:** Solve for x in

$x \equiv 1 \pmod{2}$
$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{4}$
$x \equiv 4 \pmod{5}$
$x \equiv 5 \pmod{6}$
$x \equiv 0 \pmod{7}$

x satisfies $x \equiv 1 \pmod{2}$ when $x = 1 + j \cdot 2$
$x = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23 \ldots\}$

x satisfies $x \equiv 2 \pmod{3}$ and all previous equations when $x = 5 + j \cdot 6$
$x = \{5, \underline{11}, 17, \underline{23}, 29, 35, 41, \underline{47} \ldots\}$

x satisfies $x \equiv 3 \pmod{4}$ and all previous equations when $x = 11 + j \cdot 12$
$x = \{\underline{11}, \underline{23}, \underline{35}, \underline{47}, 59, 71, 83, 95, 107, 119, 131, 143, 155, 167, 179, \ldots\}$

x satisfies $x \equiv 4 \pmod{5}$ and all previous equations when $x = 59 + j \cdot 60$
$x = \{59, 119, 179, \ldots\}$

x satisfies $x \equiv 5 \pmod{6}$ and all previous equations when $x = 59 + j \cdot 60$
$x = \{59, \overline{119}, 179, \ldots\}$

This equation was redundant, since $x \equiv 1 \pmod 2$ and $x \equiv 2 \pmod 3$. This says that x is an odd number one less than a multiple of three. 5 is the only odd number one less than a multiple of three in the complete canonical residue system of 6, therefore this equation is equivalent to the two previous ones.

x satisfies $x \equiv 0 \pmod 7$ and all previous equations when $x = 119 + j \cdot 420$
$x = \{\overline{119}, 539, 959, 1379, 1799, 2219, \dots\}$

3.27 **Theorem:** Let $a, b, m, n \in \mathbb{Z}$ where $m > 0$ and $n > 0$. The system $x \equiv a \pmod n$ and $x \equiv b \pmod m$ has solutions for x if and only if $\gcd(n, m) \mid (a - b)$

Proof: $x \equiv a \pmod m$, or equivalently $m \mid (x - a)$, or equivalently, $cm = x - a$, and by the same logic $dn = x - b$. Adding the system of equations together, $cm - dn = x - a - (x - b)$, or equivalently $cm - dn = a - b$. By Theorem 1.48, this has solutions if and only if $\gcd(m, n) \mid (a - b)$.

3.28 **Theorem:** Let $a, b, m, n \in \mathbb{Z}$ where $m > 0$, $n > 0$, and $\gcd(m, n) = 1$

Proof: Repeat the previous proof up to $cm - dn = a - b$. c has solutions every $\frac{n}{\gcd(m,n)} = n$ and d has solutions every $\frac{m}{\gcd(m,n)} = m$. $a + cm = x$ and $b + dn = x$. $x = a + m(c_0 + in) = a + mc_0 + inm$ and $x = b + n(d_0 + im) = b + nd_0 + inm$. Solving for x in terms of c and solving for x in terms of d both indicate solutions every nm. Therefore they are equivalent to the same thing $\pmod{mn}$.

3.29 **Theorem:** Given L linear congruences with coprime modulos, there exists a unique solution in the canonical residue system of the product of the modulos.

$i \neq j \rightarrow \gcd(n_i, n_j) = 1$

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_L \pmod{n_L} \end{aligned}$$

Proof: For $L = 2$, there is a unique solution mod $n_1 n_2$ by theorem 3.28. Assume that for $L - 1$ linear congruences, there is a unique solution mod $n_1 n_2 \dots n_{L-1}$, called k_{L-1}. Then to satisfy all of the previous $L - 1$ equations $x \equiv k_{L-1} \pmod{n_1 n_2 \dots n_{L-1}}$. Add on to this that $x \equiv a_L \pmod{n_L}$. These two equations have a unique solution mod $n_1 n_2 \dots n_{L-1} n_L$ by theorem 3.28. By induction, the L equations have solutions every $n_1 n_2 \dots n_{L-1} n_L$. ■