



Foundations of Computing I

* All slides are a combined effort between previous instructors of the course

Large Non-negative Integer Operations MOD M

Exponentiation?

$a \equiv 0 \pmod{m}$
 $(a \cdot b \cdot c + d) \pmod{m}$

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

a	a ¹	a ²	a ³	a ⁴	a ⁵	a ⁶
1						
2						
3						
4						
5						
6						

$a^b \pmod{m}$
 $a^2 = (a^1)^2 = (a^2)^1 \dots$
 $a^5 = a \cdot a^4 = a \cdot (a^2)^2$

Exponentiation

- Compute 78365^{81453}
- Compute $78365^{81453} \pmod{104729}$
- Output is small
 - need to keep intermediate results small

Repeated Squaring – small and fast

Since $a \pmod{m} \equiv a \pmod{m}$ for any a
 we have $a^2 \pmod{m} = (a \pmod{m})^2 \pmod{m}$
 and $a^4 \pmod{m} = (a^2 \pmod{m})^2 \pmod{m}$
 and $a^8 \pmod{m} = (a^4 \pmod{m})^2 \pmod{m}$
 and $a^{16} \pmod{m} = (a^8 \pmod{m})^2 \pmod{m}$
 and $a^{32} \pmod{m} = (a^{16} \pmod{m})^2 \pmod{m}$

Can compute $a^k \pmod{m}$ for $k=2^i$ in only i steps

Fast Exponentiation Algorithm

$$81453 = 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^5 + 2^3 + 2^2 + 2^0$$

$$a^{81453} = a^{2^{16}} \cdot a^{2^{13}} \cdot a^{2^{12}} \cdot a^{2^{11}} \cdot a^{2^{10}} \cdot a^{2^9} \cdot a^{2^5} \cdot a^{2^3} \cdot a^{2^2} \cdot a^{2^0}$$

$$a^{81453} \pmod{m} = (\dots((((a^{2^{16}} \pmod{m} \cdot a^{2^{13}} \pmod{m}) \pmod{m} \cdot a^{2^{12}} \pmod{m}) \pmod{m} \cdot a^{2^{11}} \pmod{m}) \pmod{m} \cdot a^{2^{10}} \pmod{m}) \pmod{m} \cdot a^{2^9} \pmod{m}) \pmod{m} \cdot a^{2^5} \pmod{m}) \pmod{m} \cdot a^{2^3} \pmod{m}) \pmod{m} \cdot a^{2^2} \pmod{m}) \pmod{m} \cdot a^{2^0} \pmod{m}) \pmod{m}$$

The fast exponentiation algorithm computes $a^n \pmod{m}$ using $O(\log n)$ multiplications mod m

Fast Exponentiation

```
public static long FastModExp(long base, long exponent, long modulus) {
    long result = 1;
    base = base % modulus;

    while (exponent > 0) {
        if ((exponent % 2) == 1) {
            result = (result * base) % modulus;
            exponent -= 1;
        }
        /* Note that exponent is definitely divisible by 2 here. */
        exponent /= 2;
        base = (base * base) % modulus;
        /* The last iteration of the loop will always be exponent = 1 */
        /* so, result will always be correct. */
    }
    return result;
}
```

$a^n = a^{2^k} \rightarrow (a^2)^k$
 $a^{2^k n} \rightarrow a \cdot (a^2)^k$

Large Non-negative Integer Operations MOD M

Division?

$$\left(\frac{1}{5}\right) \cdot 5 = \frac{5}{5} = 1$$

Let's get existential.

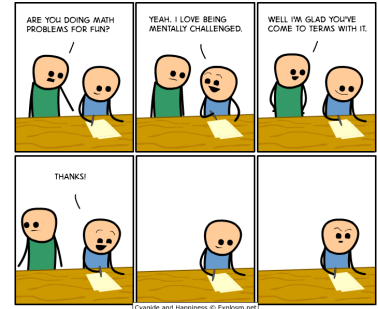
What, really, IS division?

$$5 \cdot \frac{1}{2} = \frac{5}{2} = "5/2" \quad \left| \quad 2x \equiv 1 \pmod{2}\right.$$

$$2x = 5$$

CSE 311: Foundations of Computing

Lecture 13: Modular Inverses



Greatest Common Divisor

GCD(a, b):

Largest integer d such that $d \mid a$ and $d \mid b$

$$100 = 2^2 \cdot 5^2 \quad 125 = 5^3 \cdot 2^0$$

- $\text{GCD}(100, 125) = 2^0 \cdot 5^2 = 25$
- $\text{GCD}(17, 49) =$
- $\text{GCD}(11, 66) =$
- $\text{GCD}(13, 0) =$
- $\text{GCD}(180, 252) =$

GCD and Factoring

$$a = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 = 46,200$$

$$b = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 = 204,750$$

$$\text{GCD}(a, b) = 2^{\min(3,1)} \cdot 3^{\min(1,2)} \cdot 5^{\min(2,3)} \cdot 7^{\min(1,1)} \cdot 11^{\min(1,0)} \cdot 13^{\min(0,1)}$$

Factoring is expensive!

Can we compute $\text{GCD}(a,b)$ without factoring?

Useful GCD Fact

If a and b are positive integers, then
 $\text{gcd}(a,b) = \text{gcd}(b, a \bmod b)$

Let $a, b \in \mathbb{Z}^+$ (1) $F_{a,b} \subseteq F_{b, a \bmod b}$

$F_{a,b} \rightarrow F_{b, a \bmod b}$

Suppose $x \in F_{a,b}$ is arbitrary.
 So, $x \mid a$ and $x \mid b$.
 So, $a = kx$ and $b = lx$
 $kx - lx(a \div b) = a - b(a \div b) = (a \bmod b)$
 So, $x \mid (a \bmod b)$
 So, $x \in F_{b, a \bmod b}$

By division theorem,
 $a = b \cdot (a \div b) + a \bmod b$
 $a \bmod b = a - b \cdot (a \div b)$

Useful GCD Fact

If a and b are positive integers, then
 $\text{gcd}(a,b) = \text{gcd}(b, a \bmod b)$

Proof:

By definition of mod, $a = qb + (a \bmod b)$ for some integer $q = a \div b$.

Let $d = \text{gcd}(a,b)$. Then $d \mid a$ and $d \mid b$ so $a = kd$ and $b = jd$ for some integers k and j .

Therefore $(a \bmod b) = a - qb = kd - qjd = d(k - qj)$.

So, $d \mid (a \bmod b)$ and since $d \mid b$ we must have $d \leq \text{gcd}(b, a \bmod b)$.

Now, let $e = \text{gcd}(b, a \bmod b)$. Then $e \mid b$ and $e \mid (a \bmod b)$. It follows that $b = me$ and $(a \bmod b) = ne$ for some integers m and n . Therefore

$$a = qb + (a \bmod b) = qme + ne = e(qm + n)$$

So, $e \mid a$ and since $e \mid b$ we must have $e \leq \text{gcd}(a, b)$.

Therefore $\text{gcd}(a, b) = \text{gcd}(b, a \bmod b)$.

Euclid's Algorithm

If a and b are positive integers, then
 $\gcd(a, b) = \gcd(b, a \bmod b)$

GCD Algorithm

$\gcd(a, 0) = a$
 $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\begin{aligned} \gcd(126, 660) &= \gcd(660, 126) \\ &= \gcd(126, 660 \bmod 126) \end{aligned}$$

Euclid's Algorithm

If a and b are positive integers, then
 $\gcd(a, b) = \gcd(b, a \bmod b)$

GCD Algorithm

$\gcd(a, 0) = a$
 $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\begin{aligned} \gcd(126, 660) &= \gcd(660, 660 \bmod 126) \\ &= \gcd(660, 126) \\ &= \gcd(126, 660 \bmod 126) \\ &= \gcd(126, 30) \\ &= \gcd(30, 126 \bmod 60) \\ &= \gcd(30, 6) \\ &= \gcd(6, 30 \bmod 6) \\ &= \gcd(6, 0) \\ &= 6 \end{aligned}$$

Euclid's Algorithm

GCD Algorithm

$\gcd(a, 0) = a$
 $\gcd(a, b) = \gcd(b, a \bmod b)$

```
gcd(a, b) {
  if (b == 0) {
    return a;
  }
  else {
    return gcd(b, a mod b);
  }
}
```

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that
 $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$\gcd(a, 0) = a$
 $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\begin{aligned} 5x &= 1 \quad (\text{mod } 6) \\ \hookrightarrow 5x + 6y &= 1 \end{aligned}$$

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$\gcd(a, 0) = a$
 $\gcd(a, b) = \gcd(b, a \bmod b)$

Case 1: $\gcd(a, 0) = a$

$$\begin{aligned} \gcd(a, 0) &= a \cdot x_{a,0} + 0 \cdot y_{a,0} \\ &= a \cdot 1 + 0 \cdot 0 \end{aligned}$$

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$\gcd(a, 0) = a \cdot 1 + 0 \cdot 0$
 $\gcd(a, b) = \gcd(b, a \bmod b)$

Case 2: $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\gcd(a, b) = a \cdot x_{a,b} + b \cdot y_{a,b}$$

We've figured out the answer for the "base case".

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$$\gcd(a, 0) = a*1 + 0*0$$

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Case 2: $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\gcd(a, b) = ax_{a,b} + by_{a,b}$$

$$= \gcd(b, a \bmod b) = ??????????$$

We're stuck. We need to find $X_{a,b}$ and $Y_{a,b}$.

We're looking for an equation with $a*x + b*y$. The "a mod b" doesn't belong.

$$\gcd(b, a \bmod b) = bX_{b,a \bmod b} + (a \bmod b)Y_{b,a \bmod b}$$

Division Theorem

$$a = b(a \operatorname{div} b) + (a \bmod b)$$

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$$\gcd(a, 0) = a*1 + 0*0$$

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Case 2: $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\gcd(a, b) = ax_{a,b} + by_{a,b}$$

$$= \gcd(b, a \bmod b) = ??????????$$

We're stuck. We need to find $X_{a,b}$ and $Y_{a,b}$.

We're looking for an equation with $a*x + b*y$. The "a mod b" doesn't belong.

$$\gcd(b, a \bmod b) = bX_{b,a \bmod b} + (a \bmod b)Y_{b,a \bmod b}$$

$$= bX_{b,a \bmod b} + (a - b(a \operatorname{div} b))Y_{b,a \bmod b}$$

Division Theorem

$$a = b(a \operatorname{div} b) + (a \bmod b)$$

$$(a \bmod b) = a - b(a \operatorname{div} b)$$

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$$\gcd(a, 0) = a*1 + 0*0$$

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Case 2: $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\gcd(a, b) = ax_{a,b} + by_{a,b}$$

$$= \gcd(b, a \bmod b) = ??????????$$

$$\gcd(b, a \bmod b) = bX_{b,a \bmod b} + (a \bmod b)Y_{b,a \bmod b}$$

$$= bX_{b,a \bmod b} + (a - b(a \operatorname{div} b))Y_{b,a \bmod b}$$

We're still looking for $X_{a,b}$ and $Y_{a,b}$. The equation has x and y terms. Group them...

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$$\gcd(a, 0) = a*1 + 0*0$$

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Case 2: $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\gcd(a, b) = ax_{a,b} + by_{a,b}$$

$$= \gcd(b, a \bmod b) = ??????????$$

$$\gcd(b, a \bmod b) = bX_{b,a \bmod b} + (a \bmod b)Y_{b,a \bmod b}$$

$$= bX_{b,a \bmod b} + (a - b(a \operatorname{div} b))Y_{b,a \bmod b}$$

We're still looking for $X_{a,b}$ and $Y_{a,b}$. The equation has x and y terms. Group them...

$$= bX_{b,a \bmod b} + aY_{b,a \bmod b} - b(a \operatorname{div} b)Y_{b,a \bmod b}$$

$$= b(X_{b,a \bmod b} - (a \operatorname{div} b)Y_{b,a \bmod b}) + aY_{b,a \bmod b}$$

$$= aY_{b,a \bmod b} + b(X_{b,a \bmod b} - (a \operatorname{div} b)Y_{b,a \bmod b})$$

$$\gcd(b, a \bmod b) = aY_{b,a \bmod b} + b(X_{b,a \bmod b} - (a \operatorname{div} b)Y_{b,a \bmod b})$$

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$$\gcd(a, 0) = a*1 + 0*0$$

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Case 2: $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\gcd(a, b) = ax_{a,b} + by_{a,b}$$

$$= \gcd(b, a \bmod b)$$

$$= aY_{b,a \bmod b} + b(X_{b,a \bmod b} - (a \operatorname{div} b)Y_{b,a \bmod b})$$

Finding x & y

Bézout's Theorem

If a and b are positive integers, then there exist integers $x_{(a,b)}$ and $y_{(a,b)}$ such that $\gcd(a, b) = ax_{(a,b)} + by_{(a,b)}$

GCD Algorithm

$$\gcd(a, 0) = a$$

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Case 2: $\gcd(a, b) = \gcd(b, a \bmod b)$

$$\gcd(a, b) = ax_{a,b} + by_{a,b}$$

$$= \gcd(b, a \bmod b)$$

$$= aY_{b,a \bmod b} + b(X_{b,a \bmod b} - (a \operatorname{div} b)Y_{b,a \bmod b})$$

EGCD Algorithm

$$\operatorname{egcd}(a, 0) = a*1 + 0*0$$

$$\operatorname{egcd}(a, b) = a*Y_{b,a \bmod b} + b*(X_{b,a \bmod b} - (a \operatorname{div} b)Y_{b,a \bmod b})$$

Finding x & y

GCD Algorithm

$$\gcd(a, 0) = a$$

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

EGCD Algorithm

$$\text{egcd}(a, 0) = a*1 + 0*0$$

$$\text{egcd}(a, b) = a*Y_{b,a \bmod b} + b*(X_{b,a \bmod b} - (a \text{ div } b)Y_{b,a \bmod b})$$

EGCD Algorithm

$$\text{egcd}(a, 0) = (a, 1, 0)$$

$$\text{egcd}(a, b) = (\gcd(b, a \bmod b), Y_{b,a \bmod b}, X_{b,a \bmod b} - (a \text{ div } b)*Y_{b,a \bmod b})$$

Computing x & y By Hand

EGCD Algorithm

$$\text{egcd}(a, 0) = (a, 1, 0)$$

$$\text{egcd}(a, b) = (\gcd(b, a \bmod b), Y_{b,a \bmod b}, X_{b,a \bmod b} - (a \text{ div } b)*Y_{b,a \bmod b})$$

Find x and y such that $\gcd(35, 27) = 35*x + 27*y$

a	b	a mod b	a div b	$\gcd(a,b) = a * x + b * y$
35	27	8	1	= 35 * + 27 *
				= * + *
				= * + *
				= * + *
				= * + *
				= * + *

We fill in this table row by row. First, we fill in all the left side. Then, we fill in the right side on our way back up.

Computing x & y By Hand

EGCD Algorithm

$$\text{egcd}(a, 0) = (a, 1, 0)$$

$$\text{egcd}(a, b) = (\gcd(b, a \bmod b), Y_{b,a \bmod b}, X_{b,a \bmod b} - (a \text{ div } b)*Y_{b,a \bmod b})$$

Find x and y such that $\gcd(35, 27) = 35*x + 27*y$

a	b	a mod b	a div b	$\gcd(a,b) = a * x + b * y$
35	27	8	1	= 35 * + 27 *
27	8			= 27 * + 8 *
				= * + *
				= * + *
				= * + *
				= * + *

Since $\gcd(a,b) = \gcd(b, a \bmod b)$, we copy down b and a mod b.

Computing x & y By Hand

EGCD Algorithm

$$\text{egcd}(a, 0) = (a, 1, 0)$$

$$\text{egcd}(a, b) = (\gcd(b, a \bmod b), Y_{b,a \bmod b}, X_{b,a \bmod b} - (a \text{ div } b)*Y_{b,a \bmod b})$$

Find x and y such that $\gcd(35, 27) = 35*x + 27*y$

a	b	a mod b	a div b	$\gcd(a,b) = a * x + b * y$
35	27	8	1	= 35 * + 27 *
27	8	3	3	= 27 * + 8 *
8	3	2	2	= 8 * + 3 *
3	2	1	1	= 3 * + 2 *
2	1	0	2	= 2 * + 1 *
1	0			= 1 * + 0 *

We got to $\gcd(a, 0) = a$. So, fill in $\gcd(a, b)$ all the way up.

Computing x & y By Hand

EGCD Algorithm

$$\text{egcd}(a, 0) = (a, 1, 0)$$

$$\text{egcd}(a, b) = (\gcd(b, a \bmod b), Y_{b,a \bmod b}, X_{b,a \bmod b} - (a \text{ div } b)*Y_{b,a \bmod b})$$

Find x and y such that $\gcd(35, 27) = 35*x + 27*y$

a	b	a mod b	a div b	$\gcd(a,b) = a * x + b * y$
35	27	8	1	1 = 35 * + 27 *
27	8	3	3	1 = 27 * + 8 *
8	3	2	2	1 = 8 * + 3 *
3	2	1	1	1 = 3 * + 2 *
2	1	0	2	1 = 2 * + 1 *
1	0			1 = 1 * + 0 *

Now, we back-fill X and Y using the equation for egcd:

- $X_n = Y_{n+1}$
- $Y_n = X_{n+1} - (a \text{ div } b)*Y_{n+1}$

Computing x & y By Hand

EGCD Algorithm

$$\text{egcd}(a, 0) = (a, 1, 0)$$

$$\text{egcd}(a, b) = (\gcd(b, a \bmod b), Y_{b,a \bmod b}, X_{b,a \bmod b} - (a \text{ div } b)*Y_{b,a \bmod b})$$

Find x and y such that $\gcd(35, 27) = 35*x + 27*y$

a	b	a mod b	a div b	$\gcd(a,b) = a * x + b * y$
35	27	8	1	1 = 35 * + 27 *
27	8	3	3	1 = 27 * + 8 *
8	3	2	2	1 = 8 * + 3 *
3	2	1	1	1 = 3 * + 2 *
2	1	0	2	1 = 2 * + 1 *
1	0			1 = 1 * 1 + 0 * 0

Computing x & y By Hand

EGCD Algorithm

$$\text{egcd}(a, 0) = (a, 1, 0)$$

$$\text{egcd}(a, b) = (\text{gcd}(b, a \bmod b), Y_{b, a \bmod b}, X_{b, a \bmod b} - (a \text{ div } b) * Y_{b, a \bmod b})$$

Find x and y such that $\text{gcd}(35, 27) = 35*x + 27*y$

a	b	a mod b	a div b	gcd(a,b)	= a * x + b * y
35	27	8	1	1	= 35 * + 27 * *
27	8	3	3	1	= 27 * + 8 * *
8	3	2	2	1	= 8 * + 3 * *
3	2	1	1	1	= 3 * + 2 * *
2	1	0	2	1	= 2 * 0 + 1 * 1
1	0			1	= 1 * 1 + 0 * 0

Computing x & y By Hand

EGCD Algorithm

$$\text{egcd}(a, 0) = (a, 1, 0)$$

$$\text{egcd}(a, b) = (\text{gcd}(b, a \bmod b), Y_{b, a \bmod b}, X_{b, a \bmod b} - (a \text{ div } b) * Y_{b, a \bmod b})$$

Find x and y such that $\text{gcd}(35, 27) = 35*x + 27*y$

a	b	a mod b	a div b	gcd(a,b)	= a * x + b * y
35	27	8	1	1	= 35 * -10 + 27 * 13
27	8	3	3	1	= 27 * 3 + 8 * -10
8	3	2	2	1	= 8 * -1 + 3 * 3
3	2	1	1	1	= 3 * 1 + 2 * -1
2	1	0	2	1	= 2 * 0 + 1 * 1
1	0			1	= 1 * 1 + 0 * 0

$$\text{So, } 1 = \text{gcd}(35, 27) = 35*(-10) + 27*13$$

Large Non-negative Integer Operations MOD M

Division?

FINALLY! We're back to division mod m.

In normal arithmetic, if I multiply $x * (1/x)$, I get back x.

In MODULAR arithmetic, if I multiply $x * ?$, I get back x.

"1/x" is the unique number that, when multiplied by x gives 1.

"1/x" is a solution, N, to the equation $xN \equiv 1 \pmod{m}$.

$$\begin{aligned} xN \equiv 1 \pmod{m} &\leftrightarrow m \mid (xN - 1) \\ &\leftrightarrow xN - 1 = km \\ &\leftrightarrow xN + (-k)m = 1 \end{aligned}$$

We know how to do this now! It's just EGCD!

Large Non-negative Integer Operations MOD M

Division?

FINALLY! We're back to division mod m.

In normal arithmetic, if I multiply $x * (1/x)$, I get back x.

In MODULAR arithmetic, if I multiply $x * ?$, I get back x.

"1/x" is the unique number that, when multiplied by x gives 1.

Example

Solve: $7x \equiv 1 \pmod{26}$

Example

Solve: $7x \equiv 1 \pmod{26}$

$$\text{gcd}(26, 7) = \text{gcd}(7, 5) = \text{gcd}(5, 2) = \text{gcd}(2, 1) = 1$$

$$26 = 7*3 + 5$$

$$5 = 26 - 7*3$$

$$7 = 5*1 + 2$$

$$2 = 7 - 5*1$$

$$5 = 2*2 + 1$$

$$1 = 5 - 2*2$$

$$\begin{aligned} 1 &= 5 - (7 - 5*1)*2 \\ &= (-7)*2 + 5*3 \\ &= (-7)*2 + (26 - 7*3)*3 \\ &= 7*(-11) + 26*3 \end{aligned}$$

So, $x = 15 + 26k$ for $k \in \mathbb{N}$.