Lecture Notes

Keshav Ramamurthy

February 11, 2026

Contents

1 **2**

2 **2**

3 Modular Practice **2**

3.1 (a) 2

3.2 (b) 2

3.3 (c) 2

3.4 (d) 2

3.5 (e) 3

4 Wilson's Theorem **3**

1

2

3 Modular Practice

3.1 (a)

notice

$$9x + 5 \equiv 7 \mod 13 \to 9x \equiv 7 - 5 \mod 13 \to 9x \equiv 2 \mod 13$$

then, notice that $9 \cdot 3 \equiv 27 \equiv 1 \mod 13$, so multiplying by 3 on both sides yields

$$9 \cdot 3 \cdot x \equiv 2 \cdot 3 \mod 13 \to \boxed{x \equiv 6 \mod 13}$$

3.2 (b)

notice

$$3x + 12 \equiv 4 \mod 21 \to 3x \equiv -8$$

then, we have that

$$3x \equiv 13 \mod 21$$

then, since the lhs is divisible by 3, notice that since the rhs is 13 mod 21, that this is equivalent to

$$21w + 13 \equiv 1 \mod 3$$

because the rhs and lhs have different parities mod 3, there are no solutions $\square$

3.3 (c)

let's write the systems first

$$5x + 4y \equiv 0 \mod 7$$

$$2x + y \equiv 4 \mod 7$$

notice that $y \equiv 4 - 2x \mod 7$, and that thus we can substitute that into the top equation yielding

$$5x + 4(4 - 2x) \equiv 0 \mod 7 \to -3x + 16 \equiv 0 \mod 7 \to 3x \equiv 16 \mod 7 \to 3 \cdot 5 \cdot x \equiv 16 \cdot 5 \mod 7$$

This reduces to $x \equiv 3 \mod 7$ yielding $y \equiv 4 - 2x \equiv 5 \mod 7$

3.4 (d)

Notice

$$(13)^{2023} = (12 + 1)^{2023} \equiv (0 + 1)^{2023} \equiv 1^{2023} \equiv 1 \mod 7$$

3.5 (e)

By Fermat's little theorem, since 11 is prime, we have that

$$7^{11-1} = 7^{10} \equiv 1 \mod 11$$

Then,

$$7^{62} \equiv 7^{60}7^2 \equiv \left(7^{10}\right)^6 7^2 \equiv 7^2 \equiv 5 \mod 11$$

4 Wilson's Theorem

Let us first show that if p is prime, that this holds. Then, we will prove the other direction We'll first show every residue r mod p except 0 has an inverse mod p. Notice if r has an inverse

$$\exists r^{-1} \in (\mathbb{Z}/p\mathbb{Z})^{\times} \mid rr^{-1} \equiv 1 \mod p$$

We know that every number $r \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ has an inverse by Bezout's identity, since $\gcd(r, p) = 1$. We claim that that the pairs

$$(1, 1), (p-1, p-1) \left(r_1, r_1^{-1}\right), \left(r_2, r_2^{-1}\right), \left(r_3, r_3^{-1}\right), \cdots, \left(r_{\frac{p-3}{2}}, r_{\frac{p-3}{2}}^{-1}\right)$$

contain all the numbers in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ exactly once(except for 1 and $p-1$)
Notice for any residue r, that it's inverse must be unique, as if r had two inverses i_1^{-1}, i_2^{-1}, then we'd have that

$$ri_1^{-1} \equiv ri_2^{-1} \equiv 1 \to r\left(i_1^{-1} - i_s^{-1}\right) \equiv 0 \to i_1^{-1} = i_2^{-1}$$

which is false my contradiction. However, it's inverse may not be distinct from r, so let's examine the case that $r \cdot r \equiv 1 \mod p$
Notice this turns into

$$r^2 - 1 \equiv 0 \mod p \to r \equiv 1, -1 \mod p$$

So, two of our pairs are $(1, 1)$ and $(p-1, p-1)$, but the rest are distinct, which then contain $(\mathbb{Z}/p\mathbb{Z})^{\times}$
Thus, if every residue r must have a unique inverse, and an inverse exists for every residue, they have to pair up and contain all the numbers in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ Now, notice that

$$(p-1)! \equiv \prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{\frac{p-3}{2}} \left(r_i r_i^{-1}\right) \cdot 1 \cdot (p-1) \equiv (1)^{\frac{p-3}{2}} \cdot 1 \cdot -1 \equiv -1 \mod p \quad \square$$