

Abstract Algebra by Pinter, Chapter 23

Amir Taaki

Chapter 23 on Elements of Number Theory

Contents

A. Solving Single Congruences	3
Q1	3
a	3
b	4
c	4
d	4
e	4
f	4
Q2	4
a	4
b	4
c	5
d	5
e	5
f	5
Q3	5
a	5
b	6
Q4	6
a	6
b	6
c	6
d	6
e	6
f	6
Q5	6
a	6
b	7
c	7
d	7
Q6	7
a	7
b	7
c	7
d	7
B. Solving Sets of Congruences	8
Q1	8
a	8
b	8
c	8
Q2	9
a	9
b	9
c	10
Q3	10

Q4	10
a	10
b	11
Q5	12
a	12
b	12
C. Elementary Properties of Congruence	13
Q1	13
Q2	13
Q3	13
Q4	14
Q5	14
Q6	14
Q7	14
Q8	14
Q9	15
D. Further Properties of Congruence	15
Q1	15
Q2	15
Q3	15
Q4	16
Q5	16
Q6	16
Q7	16
Q8	16
Q9	17
E. Consequences of Fermat's Theorem	17
Q1	17
Q2	17
Q3	18
a	18
b	18
Q4	18
Q5	18
a	18
b	19
Q6	19
a	19
b	19
Q7	19
Q8	19
a	19
b	20
c	20
d	20
Q9	20
a	20
b	20
c	20
F. Consequences of Euler's Theorem	21
Q1	21
Q2	21
Q3	21
Q4	21
Q5	22
Q6	22
Q7	22

a	22
b	23
c	23
Q8	23
Q9	23

G. Wilson's Theorem, and Some Consequences 23

Q1	23
Every Finite Integral Domain is a Field	24
Remaining Elements Product is Unity	24
Q2	24
Q3	24
Q4	24
Q5	25
Q6	25
Q7	25
Q8	25
Q9	26

H. Quadratic Residues 26

Q1	26
Q2	26
Q3	26
Q4	26
Q5	26
Q6	27
a	27
b	27
Q7	27
Q8	27
$\left(\frac{30}{101}\right)$	27
$\left(\frac{10}{151}\right)$	28
$\left(\frac{15}{41}\right)$	28
$\left(\frac{14}{59}\right)$	28
$\left(\frac{379}{401}\right)$	28
Is 14 a quadratic residue modulo 59	28
Q9	28

I. Primitive Roots 28

Q1	28
Q2	29
Q3	29
6	29
10	29
12	29
14	29
15	29
Q4	30
Q5	30
Q6	30
Q7	31

A. Solving Single Congruences

Q1

a

$$60x \equiv 12 \pmod{24}$$

$$\gcd(60, 24) = 12/12$$

$$\begin{aligned}\Rightarrow 5x &\equiv 1 \pmod{2} \\ x &\equiv 3 \pmod{2}\end{aligned}$$

b

$$\begin{aligned}\gcd(42, 30) &= 6 \\ 7x &\equiv 4 \pmod{5} \\ x &\equiv 2 \pmod{5}\end{aligned}$$

c

No solution because $\gcd(49, 25) = 1$ so equation cannot be reduced.

d

$$\begin{aligned}39 &= 13 \times 3 \\ 52 &= 13 \times 2^2 \\ \gcd(39, 52) &= 13 \nmid 14\end{aligned}$$

e

$$\gcd(147, 98) = 49 \nmid 47$$

f

$$\begin{aligned}\gcd(39, 52) &= 13 \\ 3x &\equiv 2 \pmod{4} \\ x &\equiv 3\end{aligned}$$

Q2

a

$$12x \equiv 7 \pmod{25}$$

Note that $12 \perp 25$

$$\begin{aligned}12k + 25l &= 1 \\ \Rightarrow k &= -2, l = 1 \\ \Rightarrow 12 \cdot (-2) &\equiv 1 \pmod{25} \\ \Rightarrow 12 \cdot 23 &\equiv 1 \pmod{25} \\ \Rightarrow 12 \cdot 23 \cdot 7 &\equiv 7 \pmod{25} \\ \Rightarrow 12 \cdot 11 &\equiv 7 \pmod{25}\end{aligned}$$

b

$$\begin{aligned}35x &\equiv 8 \pmod{12} \\ 35 &\perp 12 \\ \Rightarrow 35 \cdot (-1) + 12 \cdot 3 &= 1 \\ \Rightarrow 35 \cdot (-1) &\equiv 1 \pmod{12} \\ \Rightarrow 35 \cdot 11 &\equiv 1 \pmod{12} \\ \Rightarrow 35 \cdot 88 &\equiv 8 \pmod{12} \\ \Rightarrow 35 \cdot 4 &\equiv 8 \pmod{12}\end{aligned}$$

c

$$15x \equiv 9 \pmod{6}$$

$$15k + 6l = 1$$

$$15 = 6(2) + 3$$

$$6 = 3(2) + 0$$

$$\gcd(15, 6) = 3$$

$$5x \equiv 3 \pmod{2}$$

$$x \equiv 1 \pmod{2}$$

$$15(1) \equiv 9 \pmod{6}$$

d

$$42x \equiv 12 \pmod{30}$$

$$42k + 30l = \gcd(42, 30)$$

$$42 = 30(1) + 12$$

$$30 = 12(2) + 6$$

$$12 = 6(2) + 0$$

$$7x \equiv 2 \pmod{5}$$

$$2x \equiv 2 \pmod{5}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 1 \pmod{30}$$

e

$$147x \equiv 49 \pmod{98}$$

$$1\bar{4}7 = \bar{4}9$$

$$\implies 49x \equiv 49 \pmod{98}$$

$$\implies x \equiv 1 \pmod{98}$$

f

$$39x \equiv 26 \pmod{52}$$

$$52 = 39(1) + 13$$

$$39 = 13(3) + 0$$

$$\implies \gcd(52, 39) = 13$$

$$\implies 3x \equiv 2 \pmod{4}$$

$$\implies x \equiv 2 \pmod{4}$$

$$\implies x \equiv 2 \pmod{52}$$

Q3

a

$$2x^2 \equiv 8 \pmod{10}$$

$$\implies 2x^2 - 8 = 10y$$

but $\gcd(2, 10) = 2$

$$\implies x^2 - 4 = 5y \in \langle 5 \rangle$$

$$\implies x^2 - 4 \equiv 0 \pmod{5}$$

$$\implies x^2 \equiv 4 \pmod{10}$$

b

$$1^2 \equiv 1 \pmod{5}$$

$$2^2 \equiv 4 \pmod{5}$$

$$3^2 \equiv 4 \pmod{5}$$

$$4^2 \equiv 1 \pmod{5}$$

Q4

a

$$\begin{aligned} 6x^2 \equiv 9 \pmod{15} &\implies 2x^2 \equiv 3 \pmod{5} \\ &\implies x \equiv 2 \pmod{5} \end{aligned}$$

b

$$\begin{aligned} 60x^2 \equiv 18 \pmod{24} &\implies 10x^2 \equiv 3 \pmod{4} \\ &\implies 2x^2 \equiv 3 \pmod{4} \end{aligned}$$

$x \neq 2$ because $2 \times 2 \mid 4 \implies x^2 \equiv 0 \pmod{4}$.

Likewise coefficient is 2 so for any n , $2n$ is either 2 or 0. No solution.

c

$$\begin{aligned} 30x^2 &\equiv 18 \pmod{24} \\ \implies 5x^2 &\equiv 3 \pmod{4} \\ \implies x^2 &\equiv 3 \pmod{4} \end{aligned}$$

No solution.

d

$$\begin{aligned} 4(x+1)^2 &\equiv 14 \pmod{10} \\ \implies 4(x+1)^2 &\equiv 4 \pmod{10} \\ x &\equiv 0 \pmod{10} \end{aligned}$$

e

$$\begin{aligned} 4x^2 - 2x + 2 &\equiv 0 \pmod{6} \\ \implies 2x^2 - x + 1 &\equiv 0 \pmod{3} \\ \implies x &= 2 \end{aligned}$$

f

$$\begin{aligned} 3x^2 - 6x + 6 &\equiv 0 \pmod{15} \\ \implies x^2 - 2x + 2 &\equiv 0 \pmod{5} \\ x &= 3, 4 \pmod{5} \end{aligned}$$

Q5

a

$$\begin{aligned} x^4 &\equiv 4 \pmod{6} \\ x^4 &\equiv (x^2)^2 \pmod{6} \end{aligned}$$

Let $y = x^2$

$$\begin{aligned} y^2 &\equiv 4 \pmod{6} \\ y &\equiv 2 \pmod{6} \text{ or } 4 \pmod{6} \\ x^2 &\equiv 2 \pmod{6} \text{ or } 4 \pmod{6} \\ \implies x &\equiv 2 \pmod{6} \end{aligned}$$

b

$$\begin{aligned}2(x-1)^4 &\equiv 0 \pmod{8} \\ \implies (x-1)^4 &\equiv 0 \pmod{4} \\ \implies (x-1)^2 &\equiv 0, 2 \pmod{4}\end{aligned}$$

Let $y = x - 1$

$$\begin{aligned}\implies y^2 &\equiv 0 \pmod{4} \\ \implies y &\equiv 0, 2 \pmod{4} \\ \implies x &\equiv 1, 3 \pmod{4}\end{aligned}$$

c

$$\begin{aligned}x^3 + 3x^2 + 3x + 1 &\equiv 0 \pmod{8} \\ (x+1)^3 &\equiv 0 \pmod{8} \\ \implies x+1 &\equiv 0, 2, 4, 6\end{aligned}$$

(any factor of 2 since $2^3 \equiv 8 \equiv 0$)

$$\implies x \equiv 7, 1, 3, 5$$

d

$$\begin{aligned}x^4 + 2x^2 + 1 &\equiv 4 \pmod{5} \\ \implies (x^2 + 1) &\equiv 4 \pmod{5} \\ \implies x^2 + 1 &\equiv 2, 3 \pmod{5} \\ \implies x^2 &\equiv 1, 2 \pmod{5} \\ \implies x &\equiv 1, 4 \pmod{5}\end{aligned}$$

Q6

a

$$14x + 15y = 11$$

Note that $14(-1) + 15(1) = 1$, thus

$$\begin{aligned}14(-1 \cdot 11) + 15(1 \cdot 11) &= 11 \\ x = -11, y &= 11\end{aligned}$$

b

$$4(-1) + 5(1) = 1$$

c

$21x + 10y$ is an ideal in \mathbb{Z} , with a least value t , such that $J = \langle t \rangle$ and therefore if $q \in J$ then $t \mid q$.

But the least value $t = 11$ and $11 \nmid 9$. So there is no solution.

d

$$\begin{aligned}30x^2 + 24y &= 18 \\ 30x^2 &\equiv 18 \pmod{24} \\ 5x^2 &\equiv 3 \pmod{4} \\ x^2 &\equiv 3 \pmod{4}\end{aligned}$$

B. Solving Sets of Congruences

Q1

a

$$x \equiv 7 \pmod{8} \quad x \equiv 11 \pmod{12}$$

$$\gcd(8, 12) = 4$$

$$7 \pmod{4} \equiv 3 \equiv 11 \pmod{4}$$

Solution exists.

$$\text{lcm}(8, 12) = 8 \times 12/4 = 24$$

$$x = 8q + 7$$

$$\implies 8q + 7 \equiv 11 \pmod{12}$$

$$8q \equiv 4 \pmod{12}$$

$$q \equiv 5 \pmod{12}$$

$$x = 8q + 7$$

$$= 8(12r + 5) + 7$$

$$= 96r + 47$$

$$x \equiv 47 \pmod{24}$$

$$\equiv 23 \pmod{24}$$

b

$$x \equiv 12 \pmod{18} \quad x \equiv 30 \pmod{45}$$

$$\gcd(18, 45) = 9$$

$$\text{lcm}(18, 45) = 18 \times 45/9 = 90$$

$$x = 18q + 12$$

$$18q + 12 \equiv 30 \pmod{45}$$

$$18q \equiv 18 \pmod{45}$$

$$q \equiv 1 \pmod{45}$$

$$x = 18(45r + 1) + 12$$

$$= 18 \times 45r + 30$$

$$x \equiv 30 \pmod{90}$$

c

$$\gcd(15, 14) = 1$$

$$\text{lcm}(15, 14) = 210$$

$$15q + 8 \equiv 11 \pmod{14}$$

$$15q \equiv 3 \pmod{14}$$

$$q \equiv 3 \pmod{14}$$

$$x \equiv 53 \pmod{210}$$

Q2

a

$$10x \equiv 2 \pmod{12} \quad 6x \equiv 14 \pmod{20}$$

$$\gcd(10, 12) = 2$$

$$5x \equiv 1 \pmod{6}$$

$$x \equiv 5 \pmod{6}$$

$$6x \equiv 14 \pmod{20}$$

$$3x \equiv 7 \pmod{10}$$

$$x \equiv 9 \pmod{10}$$

$$\gcd(6, 20) = 2$$

$$\gcd(6, 10) = 2$$

$$5 \pmod{2} = 1 = 9 \pmod{2}$$

has a solution.

$$\text{lcm}(6, 10) = 30$$

solution is modulo 30.

$$x = 6q + 5$$

$$6q + 5 \equiv 9 \pmod{10}$$

$$6q \equiv 4 \pmod{10}$$

$$3q \equiv 2 \pmod{5}$$

$$q \equiv 4 \pmod{5}$$

$$q = 5r + 4$$

$$[\text{from } \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{c}{d}}]$$

$$x = 6(5r + 4) + 5 = 30r + 29$$

$$x \equiv 29 \pmod{30}$$

b

$$4x \equiv 2 \pmod{6}$$

$$9x \equiv 3 \pmod{12}$$

$$\gcd(4, 6) = 2$$

$$\therefore 4x \equiv 2 \pmod{6} \implies 2x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{3}$$

$$\gcd(9, 12) = 3$$

$$\therefore 9x \equiv 3 \pmod{12} \implies 3x \equiv 1 \pmod{4}$$

$$x \equiv 3 \pmod{4}$$

$$\gcd(3, 4) = 1$$

$$2 \pmod{1} = 0 \neq 3 \pmod{1}$$

has no solution.

c

$$\begin{aligned}6x &\equiv 2 \pmod{8} \\ 10x &\equiv 2 \pmod{12}\end{aligned}$$

$$\begin{aligned}\gcd(6, 8) = 2 &\implies 3x \equiv 1 \pmod{4} \\ \gcd(10, 12) = 2 &\implies 5x \equiv 1 \pmod{6}\end{aligned}$$

$$\implies x \equiv 3 \pmod{4}$$

$$\implies x \equiv 5 \pmod{6}$$

$$\gcd(4, 6) = 2$$

$$3 \pmod{2} = 1 = 5 \pmod{2}$$

has a solution.

$$\text{lcm}(4, 6) = 12$$

$$x = 4q + 3$$

$$4q + 3 \equiv 5 \pmod{6}$$

$$4q \equiv 2 \pmod{6}$$

$$\gcd(4, 6) = 2$$

$$\implies 2q \equiv 1 \pmod{3}$$

$$q \equiv 2 \pmod{3}$$

$$q = 3r + 2$$

$$x = 4(3r + 2) + 3$$

$$= 12r + 11$$

$$x \equiv 11 \pmod{12}$$

Q3

See attached file `ch23b3.pdf`.

Q4

a

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

All modulo are coprime so there is a solution.

$$\text{lcm}(3, 4, 5, 7) = 3 \times 4 \times 5 \times 7 = 420$$

recursively find a solution for each equation.

$$x = 3q + 2$$

$$3q + 2 \equiv 3 \pmod{4}$$

$$3q \equiv 1 \pmod{4}$$

$$q \equiv 3 \pmod{4}$$

$$q = 4r + 3$$

$$x = 3(4r + 3) + 2$$

$$= 12r + 11$$

$$x \equiv 11 \pmod{12}$$

but also $x \equiv 1 \pmod{5}$

$$x = 12q' + 11$$

$$12q' + 11 \equiv 1 \pmod{5}$$

$$12q' \equiv 0 \pmod{5}$$

$$q' \equiv 0 \pmod{5}$$

$$q' = 5r'$$

$$\implies x = 11$$

this also fits the equation $x \equiv 4 \pmod{7}$.

b

$$6x \equiv 4 \pmod{8} \quad 10x \equiv 4 \pmod{12} \quad 3x \equiv 8 \pmod{10}$$

$$6x \equiv 4 \pmod{8} \implies 3x \equiv 2 \pmod{4} \implies x \equiv 2 \pmod{4}$$

$$10x \equiv 4 \pmod{12} \implies 5x \equiv 2 \pmod{6} \implies x \equiv 4 \pmod{6}$$

$$3x \equiv 8 \pmod{10} \implies x \equiv 6 \pmod{10}$$

$$\gcd(4, 6) = 2 \quad 2 \pmod{2} = 0 = 4 \pmod{2}$$

$$\gcd(4, 10) = 2 \quad 2 \pmod{2} = 0 = 6 \pmod{2}$$

$$\gcd(6, 10) = 2 \quad 2 \pmod{2} = 0 = 6 \pmod{2}$$

thus there is a solution x .

$$t = \text{lcm}(4, 6, 10) = \text{lcm}(\text{lcm}(4, 6), 10) = \text{lcm}(12, 10) = 60$$

Solution is modulo $t = 60$.

$$x \equiv 2 \pmod{4}$$

$$x \equiv 4 \pmod{6}$$

$$x \equiv 6 \pmod{10}$$

$$x = 4q + 2$$

$$4q + 2 \equiv 4 \pmod{6}$$

$$4q \equiv 2 \pmod{6}$$

$$q \equiv 2 \pmod{6}$$

$$q = 6r + 2$$

$$x = 4(6r + 2) + 2$$

$$= 24r + 10$$

$$24r + 10 \equiv 6 \pmod{10}$$

$$24r \equiv -4 \pmod{10}$$

$$\equiv 6 \pmod{10}$$

$$12r \equiv 3 \pmod{5}$$

$$r \equiv 4 \pmod{5}$$

$$r = 5s + 4$$

$$x = 24(5s + 4) + 10$$

$$= 120s + 106$$

$$x \equiv 106 \pmod{60}$$

$$= 46 \pmod{60}$$

Q5**a**

$$4x + 6y = 2 \implies 4x \equiv 2 \pmod{6}$$

$$9x + 12y = 3 \implies 9x \equiv 3 \pmod{12}$$

$$4x \equiv 2 \pmod{6} \implies 2x \equiv 1 \pmod{3} \implies x \equiv 2 \pmod{3}$$

$$9x \equiv 3 \pmod{12} \implies 3x \equiv 1 \pmod{4} \implies x \equiv 3 \pmod{4}$$

$$x = 3q + 2$$

$$3q + 2 \equiv 3 \pmod{4}$$

$$3q \equiv 1 \pmod{4}$$

$$q \equiv 3 \pmod{4}$$

$$q = 4r + 3$$

$$x = 3(4r + 3) + 2$$

$$= 12r + 11$$

$$t = \text{lcm}(6, 12) = 12$$

$$x \equiv 11 \pmod{12}$$

$$x = 12s + 11$$

$$= -1$$

$$y = 1$$

b

$$3x + 4y = 2$$

$$5x + 6y = 2$$

$$3x + 10y = 8$$

$$3x \equiv 2 \pmod{4}$$

$$5x \equiv 2 \pmod{6}$$

$$3x \equiv 8 \pmod{10}$$

From 23B4b, $x \equiv 46 \pmod{60}$

$$6y \equiv 2 \pmod{5}$$

$$y \equiv 2 \pmod{5}$$

$$10y \equiv 8 \pmod{3}$$

$$y \equiv 2 \pmod{2}$$

$$4y \equiv 2 \pmod{3}$$

$$y \equiv 2 \pmod{3}$$

$$t = \text{lcm}(3, 5) = 15$$

$$y = 5q + 2$$

$$5q + 2 \equiv 2 \pmod{3}$$

$$2q \equiv 0 \pmod{3}$$

$$y = 2$$

but $x \equiv 46 \pmod{60}$

$$5(46) + 6(2) \equiv 50 + 12 \equiv 2 \pmod{60}$$

$$3(46) + 10(2) \equiv 18 + 20 \equiv 38 \not\equiv 8 \pmod{60}$$

so there's no solution.

C. Elementary Properties of Congruence

Q1

If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

$$b - a = nq_1$$

$$b = nq_1 + a$$

$$b - c = nq_2$$

$$(nq_1 + a) - c = nq_2$$

$$a - c = nq_2 - nq_1$$

$$= n(q_2 - q_1)$$

$$\implies a \equiv c \pmod{n}$$

Q2

If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$.

$$a - b = nq$$

$$c - c = 0$$

$$a - b + (c - c) = nq$$

$$(a + c) - (b + c) = nq$$

$$\implies a + c \equiv b + c \pmod{n}$$

Q3

If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.

$$a - b = nq$$

$$c(a - b) = cnq$$

$$ac - ab = n(qc)$$

$$ac \equiv bc \pmod{n}$$

Q4

$a \equiv b \pmod{1}$.

$$a \equiv b \pmod{n} \iff n \mid (a - b)$$

$$1 \mid (a - b) \implies a \equiv b \pmod{1}$$

Q5

If $ab \equiv 0 \pmod{p}$, where p is a prime, then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

$$ab \equiv 0 \pmod{p} \implies ab = np$$

$$\implies p \mid ab$$

but p is prime so either $p \mid a$ or $p \mid b$.

If $p \mid a$ then $a \equiv 0 \pmod{p}$.

If $p \mid b$ then $b \equiv 0 \pmod{p}$.

Q6

If $a^2 \equiv b^2 \pmod{p}$, where p is a prime, then $a \equiv \pm b \pmod{p}$.

$$a^2 \equiv b^2 \pmod{p}$$

$$a^2 - b^2 = np$$

$$(a + b)(a - b) = np$$

Since p is prime then either $p \mid (a + b)$

If $p \mid (a + b)$ then $a \equiv -b \pmod{p}$.

If $p \mid (a - b)$ then $a \equiv b \pmod{p}$.

Q7

If $a \equiv b \pmod{m}$, then $a + km \equiv b \pmod{m}$, for any integer k . In particular, $a + km \equiv a \pmod{m}$.

$$a \equiv b \pmod{m} \implies a - b = mq_1$$

$$\begin{aligned} \implies (a + km) - b &= mq_1 + km \\ &= m(q_1 + k) \end{aligned}$$

$$\implies a + km \equiv b \pmod{m}$$

$$a - a = 0 = 0m \implies a \equiv a \pmod{m}$$

$$\implies a + km \equiv a \pmod{m}$$

Q8

If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) \equiv 1$, then $a \equiv b \pmod{n}$.

$$ac \equiv bc \pmod{n} \implies ac - bc = c(a - b) = nq$$

So $n \mid c(a - b)$ but $\gcd(c, n) = 1 \implies n \mid (a - b) \implies a \equiv b \pmod{n}$.

Q9

If $a \equiv b \pmod{n}$, then $a \equiv b \pmod{m}$ for any m which is a factor of n .

$$\begin{aligned} n &= rm \\ a - b &= nq = (rm)q \\ &= m(rq) \\ \implies a &\equiv b \pmod{m} \end{aligned}$$

D. Further Properties of Congruence

Q1

If $ac \equiv bc \pmod{n}$, and $\gcd(c, n) = d$, then $a \equiv b \pmod{n/d}$.

$$\begin{aligned} ac - bc &= nq \\ \gcd(c, n) = d &\implies c = c_1d, n = n_1d \\ c_1d(a - b) &= n_1dq \\ c_1(a - b) &= n_1q \end{aligned}$$

but $\gcd(c_1, n_1) = 1$ so $n_1 \nmid c_1 \implies n_1 \mid (a - b)$.

$$\begin{aligned} \implies a - b &= n_1k \\ n = n_1d &\implies n_1 = \frac{n}{d} \\ a - b &= \left(\frac{n}{d}\right)k \\ \implies a &\equiv b \pmod{\frac{n}{d}} \end{aligned}$$

Q2

If $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

$$\begin{aligned} a_1d &\equiv b \pmod{n_1d} \\ a_1d - b &= n_1dy \\ b &= a_1d - n_1dy \\ &= d(a_1 - n_1y) \\ \implies d &\mid b \\ \gcd(a_1, n_1) = 1 &\implies \gcd(b, n_1) = 1 \\ \implies \gcd(b, n) &= d \end{aligned}$$

Q3

If $a \equiv b \pmod{p}$ for every prime p , then $a \equiv b$.

Assume $a \neq b$ and

$$\begin{aligned} a &= p_1 \cdots p_i p_{i+1} \cdots p_n \\ b &= p_1 \cdots p_i q_i \cdots q_m \end{aligned}$$

where $\gcd(a, b) = p_1 \cdots p_i$.

If $p \in \{p_1, \dots, p_i\}$ then $p \mid a$ and $p \mid b$ and $a \pmod{p} \equiv 0 \equiv b \pmod{p}$.

If $p \in \{q_1, \dots, q_m\}$ where $p \neq p_j$ such that $1 \leq j \leq n$ then $p \nmid a$ and $p \nmid b$ so $a \not\equiv b \pmod{p}$.

Likewise for $p = p_j : i < j \leq n$.

Therefore $a \equiv b \pmod{p}$ for all prime p implies they both share the exact same prime factors, and $a = b$.

Q4

If $a \equiv b \pmod{n}$, then $a^m \equiv bm \pmod{n}$ for every positive integer m .

$$(a - b) = nq$$

$$\begin{aligned} a &= b + nq \\ a^m &= (b + nq)^m \\ &= b^m + \binom{m}{1}b^{m-1}(nq)^1 + \dots + \binom{m-1}{m}b(nq)^{m-1} + (nq)^m \\ &\implies a^m \equiv b^m \pmod{n} \end{aligned}$$

Q5

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ where $\gcd(m, n) = 1$, then $a \equiv b \pmod{mn}$.

$$\begin{aligned} a - b &= mx = ny \\ \implies n \mid (a - b) \text{ and } m \mid (a - b) \end{aligned}$$

but $\gcd(m, n) = 1 \implies mn \mid (a - b)$

$$a \equiv b \pmod{mn}$$

Q6

If $ab \equiv 1 \pmod{c}$, $ac \equiv 1 \pmod{b}$ and $bc \equiv 1 \pmod{a}$, then $ab + bc + ac \equiv 1 \pmod{abc}$. (Assume $a, c > 0$.)

$$\begin{aligned} ab - 1 &= cq_1 \\ ac - 1 &= bq_2 \\ bc - 1 &= aq_3 \end{aligned}$$

$$(ab - 1)(ac - 1)(bc - 1) = (abc)(q_1q_2q_3)$$

$$\begin{aligned} (a^2bc - ab - ac + 1)(bc - 1) &= a^2b^2c^2 - ab^2c - abc^2 + bc - a^2bc + ab + ac - 1 \\ (a^2b^2c^2 - ab^2c - abc^2 - a^2bc) + bc + ab + ac &\equiv 1 \pmod{abc} \\ \implies ab + bc + ac &\equiv 1 \pmod{abc} \end{aligned}$$

Q7

If $a^2 \equiv 1 \pmod{2}$, then $a^2 \equiv 1 \pmod{4}$.

$$a^2 - 1 \mid 2 \implies a^2 - 1 \mid 4$$

Q8

If $a \equiv b \pmod{n}$, then $a^2 + b^2 \equiv 2ab \pmod{n^2}$, and conversely.

$$\begin{aligned} a - b &= nq \\ (a - b)^2 &= a^2 - 2ab + b^2 = n^2q^2 \\ \implies a^2 + b^2 &= 2ab \pmod{n^2} \end{aligned}$$

Q9

If $a \equiv 1 \pmod{m}$, then a and m are relatively prime.

$$a - 1 = mq$$

$$a - mq = 1$$

From 22c1 this implies $\gcd(a, m) = 1$.

E. Consequences of Fermat's Theorem

Q1

If p is a prime, find $\phi(p)$. Use this to deduce Fermat's theorem from Euler's theorem.

V_p is the set of all invertible elements in \mathbb{Z}_p .

V_p is thus a group with respect to multiplication.

Let $\bar{a} \in V_p$

$$\bar{s}\bar{a} = 1$$

$$\implies sa - 1 \in \langle n \rangle$$

$$\implies sa - 1 = tn$$

$$sa - tn = 1$$

So invertible elements a in $\mathbb{Z}_n \implies a$ and n are relatively prime, and vice versa.

All cosets of $\langle n \rangle$ (except $\langle n \rangle$ itself) have a gcd of 1.

$$\mathbb{Z}_p^* = \{\bar{1}, \bar{2}, \dots, \bar{p-1}\}$$

So it follows that

$$\phi(p) = p - 1$$

Q2

If $p > 2$ is a prime and $a \not\equiv 0 \pmod{p}$, then

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\implies a^{\frac{p-1}{2} \cdot 2} \equiv x^2 \equiv 1 \pmod{p}$$

$$x^2 \equiv 1 \pmod{p} \implies x \in \{-1, 1\}$$

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

Q3

a

Let p be a prime > 2 . If $p \equiv 3 \pmod{4}$, then $(p-1)/2$ is odd.

$$\begin{aligned}
p &\equiv 3 \pmod{4} \\
p-1 &\equiv 2 \pmod{4} \\
\Rightarrow 4 &\mid [(p-1)-2] \\
\Rightarrow (p-1)-2 &= 4q \\
\Rightarrow \frac{p-1}{2} - 1 &= 2q \\
\Rightarrow \frac{p-1}{2} &\equiv 1 \pmod{2}
\end{aligned}$$

thus $\frac{p-1}{2}$ is odd.

b

Let $p > 2$ be a prime such that $p \equiv 3 \pmod{4}$. Then there is no solution to the congruence $x^2 + 1 \equiv 0 \pmod{p}$.

$$\begin{aligned}
x^2 &\equiv -1 \pmod{p} \\
x^{2 \cdot \frac{p-1}{2}} &\equiv (-1)^{\frac{p-1}{2}} \pmod{p}
\end{aligned}$$

By Fermat's theorem

$$x^{p-1} \equiv 1 \pmod{p}$$

but since $(p-1)/2$ is odd, then $(-1)^{\frac{p-1}{2}} = -1$ so there is no solution to the congruence $x^2 + 1 \equiv 0 \pmod{p}$.

Q4

Let p and q be distinct primes. Then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

$$\begin{aligned}
p^{q-1} &\equiv 1 \pmod{q} \\
q^{p-1} &\equiv 1 \pmod{p} \\
p^{q-1} - 1 &= qn \\
q^{p-1} - 1 &= pm \\
(p^{q-1} - 1)(q^{p-1} - 1) &= p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1 \\
&= (pq)(mn) \\
\Rightarrow p^{q-1} + q^{p-1} &\equiv 1 \pmod{pq}
\end{aligned}$$

Q5

Let p be a prime.

a

If, $(p-1) \mid m$, then $a^m \equiv 1 \pmod{p}$ provided that $p \nmid a$.

$$\begin{aligned}
(p-1) \mid m &\Rightarrow m = q(p-1) \\
a^m &= a^{q(p-1)} = (a^{p-1})^q
\end{aligned}$$

$$\begin{aligned}
a^{p-1} &\equiv 1 \pmod{p} \\
(a^{p-1})^q &\equiv 1^q \pmod{p} \\
a^m &\equiv 1 \pmod{p}
\end{aligned}$$

b

If, $(p-1) \mid m$, then $a^m + 1 \equiv a \pmod{pq}$ for all integers a .

If $p \mid a$ then $a^x \equiv 0 \pmod{p}$ for any x so $a^{m+1} \equiv 0 \equiv a \pmod{p}$.

Otherwise $p \nmid a$ so $a^m \equiv 1 \pmod{p} \implies a^{m+1} \equiv a \pmod{p}$

Q6

Let p and q be distinct primes.

a

If $(p-1) \mid m$ and $(q-1) \mid m$, then $a^m \equiv 1 \pmod{pq}$ for any a such that $p \nmid a$ and $q \nmid a$.

$$a^m \equiv 1 \pmod{p}$$

$$a^m \equiv 1 \pmod{q}$$

$$\gcd(p, q) = 1 \implies p \text{ and } q \text{ share no divisors}$$

$$\text{but } p \mid (a^m - 1) \text{ and } q \mid (a^m - 1) \implies pq \mid (a^m - 1)$$

$$a^m - 1 \equiv 0 \pmod{pq}$$

$$a^m \equiv 1 \pmod{pq}$$

b

If $(p-1) \mid m$ and $(q-1) \mid m$, then $a^m + 1 \equiv a \pmod{pq}$ for integers a .

Let $p \mid a$ then $a \equiv 0 \pmod{p}$ and $a \equiv 1 \pmod{q}$.

$$\implies a^m(a-1) = (pq)(mn)$$

$$\implies a^{m+1} - a = (pq)(mn)$$

$$\implies a^{m+1} \equiv a \pmod{pq}$$

Likewise if $q \mid a$.

If both $p \mid a$ and $q \mid a$ then $pq \mid a$ and so $a \equiv 0 \pmod{pq}$ and $a^{m+1} \equiv 0 \pmod{pq}$.

Otherwise $p \nmid a$ and $q \nmid a$ so

$$a^m \equiv 1 \pmod{pq}$$

$$\implies a^{m+1} \equiv a \pmod{pq}$$

Q7

$$\forall i \in \{1, \dots, n\}, (p_i - 1) \mid m$$

$$\implies a^{m+1} \equiv a \pmod{\prod_{i=1}^n p_i}$$

Q8

a

$$p = 7 \quad q = 19 \quad m = 18$$

$$(7-1) \mid 18 \quad (19-1) \mid 18$$

$$\implies a^{18+1} \equiv a \pmod{7 \times 19}$$

$$a^{19} \equiv a \pmod{133}$$

b

$$a \in \langle 2 \rangle, \langle 3 \rangle, \langle 11 \rangle$$

$$m = 10$$

$$\begin{aligned} q_1 = 2 \quad q_2 = 3 \quad q_3 = 11 \\ \implies a^{10} = 1 \pmod{66} \end{aligned}$$

c

$$\begin{aligned} q_1 = 5 \quad q_2 = 17 \quad q_3 = 3 \\ m = 12 \\ (5-1) \mid 12 \quad (7-1) \mid 12 \quad (3-1) \mid 12 \\ \implies a^{13} \equiv a \pmod{105} \end{aligned}$$

d

$$\begin{aligned} q_1 = 7 \quad q_2 = 13 \quad q_3 = 17 \\ m = 48 \\ (7-1) \mid 48 \quad (13-1) \mid 48 \quad (17-1) \mid 48 \\ \implies a^{49} \equiv a \pmod{1457} \end{aligned}$$

Q9

a

$$\begin{aligned} Q = \{2, 3, 5, 7\} \\ 8^{38} = 8^{2 \times 19} = (8^2)^{19} \\ \forall q \in Q, (q-1) \mid (19-1) \\ \implies a^{18+1} \equiv a \pmod{210} \end{aligned}$$

where $a = 8^2$

$$\implies x = 8^2$$

b

$$\begin{aligned} p = 7 \quad q = 19 \\ 7^{57} = (7^3)^{19} \\ m = 18 \\ (7-1) \mid m \quad (19-1) \mid m \\ a^{m+1} \equiv a \pmod{pq} \\ (7^3)^{18+1} \equiv 7^3 \pmod{7 \times 19} \\ x = 7^3 \end{aligned}$$

c

$$\begin{aligned} Q = \{2, 3, 11\} \\ 72 = 2^3 3^2 \end{aligned}$$

73 is prime so $m \neq 73$ since there is no $(p-1) \mid m : p \in Q$.

Since $(p-1) \mid m$ then $m = 72$, if $p = 11$ then $(11-1) \nmid 72$ so $m \neq 72$.

Since 5 is a prime, and there are no factorizations of 73, this has no solution.

F. Consequences of Euler's Theorem

Q1

If $\gcd(a, n) = 1$, the solution modulo n of $ax \equiv b \pmod{n}$ is $x \equiv a^{\phi(n)-1}b \pmod{n}$.

$\gcd(a, n) = 1 \implies ax \equiv b \pmod{n}$ has a solution because it is equivalent to $\bar{a}\bar{x} = \bar{b}$ in \mathbb{Z}_n . By condition 4, \bar{a} has a multiplicative inverse in \mathbb{Z}_n .

$$\bar{x} = \bar{a}^{-1}\bar{b}$$

$$\gcd(a, n) = 1 \implies 1 - sa = tn \in \langle n \rangle \implies \bar{1} = \overline{sa}$$

Let V_n be the set of invertible elements in \mathbb{Z}_n . This is a group since inverses and products remain in V_n . From condition 4, $\bar{1} = \overline{sa} \implies 1 - sa \in \langle n \rangle \implies \gcd(a, n) = 1$. So $|V_n| = \phi(n)$ which is the number of relatively prime elements in V_n .

Since V_n is a group, the identity is $\bar{1}$ and for any $\bar{a} \in V_n$, $\bar{a}^{\phi(n)} = \bar{1}$. But we have $\bar{x} = \bar{a}^{-1}\bar{b}$ and it follows that

$$\begin{aligned} \bar{a}^{-1} &= \bar{a}^{\phi(n)}\bar{a}^{-1} \\ &= \overline{a^{\phi(n)-1}} \\ \bar{x} &= \overline{a^{\phi(n)-1}b} \\ \implies x &\equiv a^{\phi(n)-1}b \pmod{n} \end{aligned}$$

Q2

If $\gcd(a, n) = 1$, then $a^{m\phi(n)} \equiv 1 \pmod{n}$ for all values of m .

$$\begin{aligned} \gcd(a, n) = 1 &\implies a^{\phi(n)} \equiv 1 \pmod{n} \\ (a^{\phi(n)})^m &\equiv 1^m \pmod{n} \\ a^{m\phi(n)} &\equiv 1 \pmod{n} \end{aligned}$$

Q3

If $\gcd(m, n) = \gcd(a, mn) = 1$, then $a^{\phi(m)\phi(n)} \equiv 1 \pmod{mn}$.

$$\begin{aligned} a^{k\phi(m)} &\equiv 1 \pmod{m} \\ a^{l\phi(n)} &\equiv 1 \pmod{n} \end{aligned}$$

$$\begin{aligned} a^{\phi(m)\phi(n)} &\equiv 1 \pmod{m} \\ a^{\phi(m)\phi(n)} &\equiv 1 \pmod{n} \end{aligned}$$

Since $\gcd(m, n) = 1$, then by theorem 4 $t = \text{lcm}(m, n) = mn$.

$$\begin{aligned} m \mid (a^{\phi(m)\phi(n)} - 1) \text{ and } n \mid (a^{\phi(m)\phi(n)} - 1) &\iff t \mid (a^{\phi(m)\phi(n)} - 1) \\ \implies a^{\phi(m)\phi(n)} &\equiv 1 \pmod{mn} \end{aligned}$$

Q4

If p is a prime, $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$.

HINT: For any integer a , a and p^n have a common divisor $\neq \pm 1$ iff a is a multiple of p . There are exactly p^{n-1} multiples of p between 1 and p^n .

p is a prime and the only possible values for $\gcd(a, p^n)$ are p, p^2, \dots, p^n .

Therefore $p \mid a$ and a is a multiple of p .

There are p^{n-1} multiples of p between 1 and p^n because there are p^{n-1} values in the sequence

$$p, 2p, 3p, \dots, (p^{n-1})p$$

Therefore $\phi(p^n)$ is equal to the total number of values minus the total number of multiples of p (the only possible values that divide a).

$$\begin{aligned}\phi(p^n) &= p^n - p^{n-1} \\ &= p^{n-1}(p - 1)\end{aligned}$$

Q5

For every $a \not\equiv 0 \pmod{p}$, $a^{p^n(p-1)}$ (? - malformed question), where p is a prime.

$$\begin{aligned}a \not\equiv 0 \pmod{p} &\implies \gcd(a, p) = 1 \\ a^{\phi(p^n)} &\equiv 1 \pmod{p^n} \implies \gcd(a, p^n) = 1\end{aligned}$$

but $\phi(p^n) = p^{n-1}(p - 1)$ so $a^{\phi(p^n)} = a^{p^{n-1}(p-1)}$ but $a^{\phi(p^n)} \equiv 1 \pmod{p^n}$ so $a^{p^{n-1}(p-1)} \equiv 1 \pmod{p^n}$ and so also $(a^{p^{n-1}(p-1)})^p \equiv 1^p \pmod{p^n}$ or

$$a^{p^n(p-1)} \equiv 1 \pmod{p^n}$$

Q6

Under the conditions of part 3, if t is a common multiple of $\phi(m)$ and $\phi(n)$, then $a^t \equiv 1 \pmod{mn}$. Generalize to three integers l, m , and n .

$$\gcd(m, n) = \gcd(a, mn) = 1, \quad a^{\phi(m)\phi(n)} \equiv 1 \pmod{mn}$$

$$\begin{aligned}\phi(mn) &= \phi(m)\phi(n) \\ \gcd(\phi(m), \phi(n)) \cdot \text{lcm}(\phi(m), \phi(n)) &= \phi(m)\phi(n) \\ t = \text{lcm}(\phi(m), \phi(n)) &= \frac{\phi(m)\phi(n)}{\gcd(\phi(m), \phi(n))}\end{aligned}$$

$$\begin{aligned}a^t &\equiv a^{\frac{\phi(m)\phi(n)}{\gcd(\phi(m), \phi(n))}} \equiv (a^{\phi(m)\phi(n)})^{\frac{1}{\gcd(\phi(m), \phi(n))}} \\ &\equiv 1 \pmod{mn}\end{aligned}$$

Likewise for l, m, n because $\gcd(\phi(l), \phi(m), \phi(n)) = \gcd(\phi(l), \gcd(\phi(m), \phi(n)))$ and the same for lcm.

Q7

a

$$180 = 2^2 3^2 5$$

$$\begin{aligned}\phi(180) &= \phi(2^2)\phi(3^2)\phi(5) \\ &= 2^{2-1}(2-1)3^{2-1}(3-1)(5-1) \\ &= (2)(3 \times 2)(4) = (2)(6)(4)\end{aligned}$$

Note $\gcd(2^2 3^2, 5) = 1$

$$\begin{aligned}a^{\text{lcm}(\phi(2^2 3^2), \phi(5))} &\equiv 1 \pmod{180} \\ a^{\text{lcm}(12, 4)=12} &\equiv 1 \pmod{180}\end{aligned}$$

b

$$\begin{aligned}a^4 2 &\equiv 1 \pmod{1764} \\ 1764 &= 2^2 3^2 7^2 \\ \gcd(2^2, 3^2, 7^2) &= 1 \\ \text{lcm}(\phi(2^2), \phi(3^2), \phi(7^2)) &= 42 \\ a^{42} &\equiv 1 \pmod{1764}\end{aligned}$$

c

$$\begin{aligned}1800 &= 2^3 3^2 5^2 \\ \gcd(2^3, 3^2, 5^2) &= 1 \\ \text{lcm}(\phi(2^3), \phi(3^2), \phi(5^2)) &= 60 \\ a^{60} &\equiv 1 \pmod{1800}\end{aligned}$$

Q8

If $\gcd(m, n) = l$, prove that $n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{mn}$.

$$\begin{aligned}n^{\phi(m)} &\equiv 1 \pmod{m} \implies n^{\phi(m)} - 1 = mq_1 \\ m^{\phi(n)} &\equiv 1 \pmod{n} \implies m^{\phi(n)} - 1 = nq_2\end{aligned}$$

$$\begin{aligned}(n^{\phi(m)} - 1)(m^{\phi(n)} - 1) &= (mn)(q_1 q_2) \\ &= n^{\phi(m)} m^{\phi(n)} - n^{\phi(m)} - m^{\phi(n)} + 1 \\ n^{\phi(m)} m^{\phi(n)} &\equiv 1 \pmod{mn}\end{aligned}$$

Q9

If l, m, n are relatively prime in pairs, prove that $(mn)^{\phi(l)} + (ln)^{\phi(m)} + (lm)^{\phi(n)} \equiv 1 \pmod{lmn}$.

$$\begin{aligned}(mn)^{\phi(l)} &\equiv 1 \pmod{mn} \\ (lm)^{\phi(n)} &\equiv 1 \pmod{lm} \\ (ln)^{\phi(m)} &\equiv 1 \pmod{ln}\end{aligned}$$

$$\begin{aligned}[(mn)^{\phi(l)} - 1][(lm)^{\phi(n)} - 1][(ln)^{\phi(m)} - 1] &= (l^2 m^2 n^2)(q_1 q_2 q_3) \\ &= [(mn)^{\phi(l)}(lm)^{\phi(n)} - (lm)^{\phi(n)} - (mn)^{\phi(l)} + 1][(ln)^{\phi(m)} - 1] \\ &= (mn)^{\phi(l)}(lm)^{\phi(n)}(ln)^{\phi(m)} - (lm)^{\phi(n)}(ln)^{\phi(m)} \\ &\quad - (ln)^{\phi(m)}(mn)^{\phi(l)} + (ln)^{\phi(m)} - (mn)^{\phi(l)}(lm)^{\phi(n)} \\ &\quad + (lm)^{\phi(n)} + (mn)^{\phi(l)} - 1 \\ (mn)^{\phi(l)} + (ln)^{\phi(m)} + (lm)^{\phi(n)} &\equiv 1 \pmod{lmn}\end{aligned}$$

G. Wilson's Theorem, and Some Consequences

Q1

Prove that in \mathbb{Z}_p , $\overline{2} \cdot \overline{3} \cdots \overline{p-2} = \overline{1}$.

Firstly note $x^2 \equiv 1 \pmod{p} \implies x = \pm 1$ or that $x = \overline{1}$ or $x = \overline{p-1}$.

So the remaining nonzero integers in \mathbb{Z}_p have a multiplicative inverse since \mathbb{Z}_p is an integral domain having the cancellation property.

Every Finite Integral Domain is a Field

We show a typical element $a \neq 0$ has a multiplicative inverse.

Consider a, a^2, a^3, \dots . Since there are finite elements, the group is cyclic so we must have $a^m \equiv a^n \pmod{p}$ for some $m < n$. So $0 \equiv a^m - a^n \equiv a^m(1 - a^{n-m}) \pmod{p}$.

Since there are no zero divisors $a^m \not\equiv 0 \pmod{p}$ and hence $1 - a^{n-m} \equiv 0 \pmod{p}$

$$a(a^{n-m-1}) \equiv 1 \pmod{p}$$

Remaining Elements Product is Unity

For any $x \in \mathbb{Z}_p : x \neq \pm 1$, there is a multiplicative inverse $y \in \mathbb{Z}_p : y \neq \pm 1$. This is the set $\mathbb{Z}_p \setminus \{0, \pm 1\} = \{\bar{2}, \bar{3}, \dots, \overline{p-2}\}$, which has exactly $(p-3)/2$ pairs, where $xy = \bar{1}$, and so the product of all these pairs is 1.

$$\bar{2} \cdot \bar{3} \cdots \overline{p-2} = \bar{1}$$

Q2

Prove $(p-2)! \equiv 1 \pmod{p}$ for any prime number p .

$$(p-2)! = 2 \cdot 3 \cdots (p-2)$$

From the previous question $\bar{2} \cdot \bar{3} \cdots \overline{p-2} = \bar{1}$ in \mathbb{Z}_p .

But also $\bar{2} \cdot \bar{3} \cdots \overline{p-2} = \overline{2 \cdot 3 \cdots (p-2)} = \overline{(p-2)!}$ and so $\overline{(p-2)!} = \bar{1}$. Both terms are in the same coset for $\langle p \rangle \implies p \mid [(p-2)! - 1]$.

$$\implies (p-2)! \equiv 1 \pmod{p}$$

Q3

Prove $(p-1)! + 1 \equiv 0 \pmod{p}$ for any prime number p . This is known as Wilson's theorem.

$$(p-1) \equiv -1 \pmod{p}$$

$$(p-2)! \equiv 1 \pmod{p}$$

$$(p-1)! = (p-2)!(p-1)$$

$$(p-1)! \equiv (p-2)!(p-1) \pmod{p}$$

$$\equiv (1)(-1) \pmod{p}$$

$$\equiv -1 \pmod{p}$$

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

Q4

Prove that for any composite number $n \neq 4$, $(n-1)! \equiv 0 \pmod{n}$.

Any prime factor p of n will be a divisor of $(n-1)!$ because $p < n$ since $p \mid n$.

$$(n-1)! = (n-1) \cdots p \cdots 3 \cdot 2 \cdot 1$$

This also applies to all prime powers p^k in n , and so n itself is a factor of $(n-1)!$. Since n is composite (product of 2 or more integers).

$$(n-1)! \equiv 0 \pmod{n}$$

Q5

Prove that $[(p-1)/2]!^2 \equiv (-1)^{(p+1)/2} \pmod{p}$ for any prime $p > 2$.

$$\begin{aligned}(p-1)! + 1 &\equiv 0 \pmod{p} \\ (p-1)! &\equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p} \\ (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 &\equiv -1 \pmod{p}\end{aligned}$$

Multiply both sides by $(-1)^{(p-1)/2}$, noting that

$$((-1)^{(p-1)/2})^2 = (-1)^{p-1} = 1 \text{ for any prime } p > 2$$

(as p was specified in the question).

$$\begin{aligned}\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 &\equiv -1 \cdot (-1)^{(p-1)/2} \pmod{p} \\ \left(\frac{p-1}{2}\right)!^2 &\equiv (-1)^{(p+1)/2} \pmod{p}\end{aligned}$$

Q6

Prove that if $p \equiv 1 \pmod{4}$ then $(p+1)/2$ is odd. Conclude that $(\frac{p-1}{2})!^2 \equiv -1 \pmod{p}$.

$$\begin{aligned}p-1 &= 4q \\ p+1 &= 4q+2 \\ \frac{p+1}{2} &= 2q+1\end{aligned}$$

therefore $\frac{p+1}{2}$ is odd, so $(-1)^{(p+1)/2} = -1$.

Q7

Prove that if $p \equiv 3 \pmod{4}$ then $(p+1)/2$ is even. Conclude that $(\frac{p-1}{2})!^2 \equiv 1 \pmod{p}$.

$$\begin{aligned}p-3 &= 4q \\ p+1 &= 4q+4 \\ \frac{p+1}{2} &= 2q+2\end{aligned}$$

So $\frac{p+1}{2}$ is even and $(-1)^{(p+1)/2} = 1$.

Q8

Prove that when $p > 2$ is a prime, the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution if $p \equiv 1 \pmod{4}$.

$$p \equiv 1 \pmod{4} \implies 4 \mid (p-1)$$

From 23G6

$$\begin{aligned}\left(\frac{p-1}{2}\right)!^2 &\equiv -1 \pmod{p} \\ \therefore x &= \left(\frac{p-1}{2}\right)!\end{aligned}$$

Q9

Prove that for any prime $p > 2$, $x^2 \equiv -1 \pmod{p}$ has a solution iff $p \not\equiv 3 \pmod{4}$.

From 23E3b, there is no solution to $x^2 + 1 \equiv 0 \pmod{p}$ when $p \equiv 3 \pmod{4}$.

From 23G8, there is a solution when $p \equiv 1 \pmod{4}$.

H. Quadratic Residues

Q1

Let $h : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$ be defined by $h(\bar{a}) = \bar{a}^2$. To show this is a homomorphism, let $\bar{x}, \bar{y} \in \mathbb{Z}_p^*$, then $h(\bar{x} \bar{y}) = h(\overline{xy}) = \overline{xy}^2 = (\bar{x} \bar{y})^2 = \bar{x}^2 \bar{y}^2 = h(\bar{x})h(\bar{y})$. The kernel is $\{\pm 1\}$ because $h(\pm 1) = 1$ which is the identity element.

Q2

$$|\mathbb{Z}_p^\times| = p - 1$$

For any $\bar{a} \in \mathbb{Z}_p^\times$, $h(\bar{a}) = h(-\bar{a}) = \bar{a}^2$, so the range of h is $(p-1)/2$ elements.

$$\text{ran } h = R$$

The kernel of h is $\{\pm 1\}$ and $h(\pm 1) = 1$. So R contains the identity element. Secondly for any $\bar{x}^2, \bar{y}^2 \in R$, then $\bar{x}^2 \bar{y}^2 = \overline{xy}^2 \in R$, so R is a subgroup of \mathbb{Z}_p^\times .

By the orbit-stabilizer theorem, the number of cosets is $\frac{|\mathbb{Z}_p^\times|}{|R|} = 2$.

Finally if there is an \bar{x} such that there is no $\bar{a} \in R : \bar{a}^2 = \bar{x}$, then $\bar{x} \notin R$, but $\bar{x} = R\bar{x}$. Since $1 \in R$ and $1 \cdot x = x \in R\bar{x}$.

Q3

Question is wrong. Maybe it's asking about Euler's criterion?

Q4

$$\left(\frac{17}{23}\right) = -1$$

$$\left(\frac{3}{29}\right) = -1$$

$$\left(\frac{5}{11}\right) = 1$$

$$\left(\frac{8}{13}\right) = -1$$

$$\left(\frac{2}{23}\right) = 1$$

Q5

Prove if $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. In particular, $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$.

$$a + kp \equiv a \pmod{p}, x^2 \equiv a \pmod{p}$$

$$\implies x^2 \equiv a + kp \pmod{p}$$

$$\implies \left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$$

$$a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Q6**a**

Show the Legendre symbol is homomorphic.

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

If $a, b \in R$, then $ab \in R$, and $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$.

Otherwise if $a \in R, b \notin R$, then $ab \notin R \implies ab \in R \cdot -1$, so $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) = -1$ and vice versa.

Finally if $a, b \notin R$, then $a, b \in R \cdot -1$ and $ab \in R$, so $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) = 1$.

b

Malformed question.

$$\left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a^2}{p}\right)$$

Q7

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

From G8 and G9.

$x^2 \equiv -1 \pmod{p}$ has a solution if $p \equiv 1 \pmod{4}$.

$x^2 \equiv -1 \pmod{p}$ has no solution if $p \equiv 3 \pmod{4}$.

Q8

$$\left(\frac{30}{101}\right)$$

$$\left(\frac{30}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{5}{101}\right)\left(\frac{2}{101}\right)$$

$$\left(\frac{101}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$101 \equiv 1 \pmod{4} \implies \left(\frac{3}{101}\right) = -1$$

$$\left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1 \implies \left(\frac{5}{101}\right) = 1$$

Cannot use reciprocity rule because only works for prime > 2 .

$$\left(\frac{2}{101}\right) = -1$$

$$\therefore \left(\frac{30}{101}\right) = 1$$

$$\left(\frac{10}{151}\right)$$

$$\begin{aligned}\left(\frac{10}{151}\right) &= \left(\frac{2}{151}\right) \left(\frac{5}{151}\right) \\ 5 \equiv 1 \pmod{4} &\implies \left(\frac{5}{151}\right) = \left(\frac{151}{5}\right) = \left(\frac{1}{5}\right) = 1 \\ \left(\frac{2}{151}\right) &= 1 \\ \therefore \left(\frac{10}{151}\right) &= 1\end{aligned}$$

$$\left(\frac{15}{41}\right)$$

$$\begin{aligned}\left(\frac{15}{41}\right) &= \left(\frac{3}{41}\right) \left(\frac{5}{41}\right) \\ 41 \equiv 1 \pmod{4} &\implies \left(\frac{3}{41}\right) = \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = -1, \left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1 \\ \therefore \left(\frac{15}{41}\right) &= -1\end{aligned}$$

$$\left(\frac{14}{59}\right)$$

$$\left(\frac{14}{59}\right) = \left(\frac{2}{59}\right) \left(\frac{7}{59}\right)$$

$$\text{Both } 59 \equiv 7 \equiv 3 \pmod{4} \implies \left(\frac{7}{59}\right) = -\left(\frac{59}{7}\right) = -\left(\frac{3}{7}\right) = -(-1) = 1.$$

$$\frac{2}{59} = -1$$

$$\frac{14}{59} = -1$$

$$\left(\frac{379}{401}\right)$$

$$401 \equiv 1 \pmod{4} \implies \left(\frac{379}{401}\right) = \left(\frac{401}{379}\right) = \left(\frac{22}{379}\right) = 1$$

Is 14 a quadratic residue modulo 59

No

Q9

$x^2 \equiv 30 \pmod{101}$ is solvable. The other two are not solvable.

I. Primitive Roots

Recall that V_n is the multiplicative group of all the invertible elements in \mathbb{Z}_n . If V_n happens to be cyclic, say $V_n = \langle m \rangle$, then any integer $a \equiv m \pmod{n}$ is called a primitive root of n .

Q1

Prove that a is a primitive root of n iff the order of \bar{a} in V_n is $\phi(n)$.

$$\text{ord}(\bar{a}) = \phi(n) \implies \bar{a}^{\phi(n)} = \bar{1} \text{ in } V_n$$

This means there are $\phi(n)$ distinct powers of \bar{a} , which generate all the invertible elements of \mathbb{Z}_n^\times , that is $a \equiv m \pmod{n}$ and $V_n = \langle a \rangle$.

Q2

Prove that every prime number p has a primitive root. (HINT: For every prime p , \mathbb{Z}_p^\times is a cyclic group. The simple proof of this fact is given as Theorem 1 in Chapter 33.)

For every prime number, $\mathbb{Z}_p^\times = \{\overline{1}, \overline{2}, \dots, \overline{p-1}\}$ is a group with order $p-1$.

Thus $\forall x \in \mathbb{Z}_p^\times, x^{p-1} = \overline{1}, V_p = \langle x \rangle$.

Q3

Find primitive roots of the following integers (if there are none, say so): 6, 10, 12, 14, 15.

6

$$n = 6, \phi(6) = 2, \mathbb{Z}_6^\times = \{1, 5\}$$

1: 1

5: 5, 1

Primitive root of 6 is 5

10

$$n = 10, \phi(10) = 4, \mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$$

x x^2 x^3 x^4

1: 1

3: 3, 9, 7, 1

7: 7, 9, 3, 1

9: 9, 1

Primitive roots of 10 is 3 and 7

12

$$n = 12, \phi(12) = 4, \mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$$

1: 1

5: 5, 1

7: 7, 1

11: 11, 1

No primitive root of 12.

14

$$n = 14, \phi(14) = 6, \mathbb{Z}_{14}^\times = \{1, 3, 5, 9, 11, 13\}$$

1: 1

3: 3, 9, 13, 11, 5, 1

5: 5, 11, 13, 9, 3, 1

9: 9, 11, 1

11: 11, 9, 1

13: 13, 1

14 has primitive roots 3 and 5

15

$$n = 15, \phi(15) = 8, \mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

1: 1

2: 2, 4, 8, 1

4: 4, 1

7: 7, 4, 13, 1

8: 8, 4, 2, 1

11: 11, 1

13: 13, 4, 7, 1

14: 14, 1

There are no primitive roots modulo 15.

Q4

Suppose a is a primitive root of m . Prove: If b is any integer which is relatively prime to m , then $b \equiv a^k \pmod{m}$ for some $k \geq 1$.

$$\begin{aligned}\gcd(b, m) = 1 &\implies \bar{b} \in V_m = \langle a \rangle \\ &\implies \bar{b} = \bar{a}^k \text{ in } \mathbb{Z}_m \\ &\implies b \equiv a^k \pmod{m}\end{aligned}$$

Q5

Suppose m has a primitive root, and let n be relatively prime to $\phi(m)$. (Suppose $n > 0$.) Prove that if a is relatively prime to m , then $x^n \equiv a \pmod{m}$ has a solution.

\mathbb{Z}_m^\times is a multiplicative group with a cyclic subgroup V_m of invertible elements.

$$\forall x \in \mathbb{Z}_m^\times : \gcd(a, m) = 1 \iff a \in V_m$$

Thus $V_m = \langle g \rangle$, so $\bar{a} = \bar{g}^l$. So we want to find an $\bar{x} \in V_m$ or $\bar{x} = \bar{g}^k$ such that $\bar{x}^n = (\bar{g}^k)^n = \bar{g}^l$

$$(g^k)^n \equiv g^l \pmod{m}$$

This is equivalent to writing

$$\begin{aligned}kn &\equiv l \pmod{\phi(m)} \\ &\implies \phi(m) \mid (kn - l) \\ &\implies kn - l = q\phi(m)\end{aligned}$$

But note that since $\gcd(n, \phi(m)) = 1$ then

$$cn + d\phi(m) = 1 \text{ for some } c \text{ and } d$$

Returning to our previous statement, we have

$$kn - q\phi(m) = l$$

Since l is a linear combination of n and $\phi(m)$, then l is a multiple of the ideal J generated by $\gcd(n, \phi(m)) = 1$. Since J is the entire group of \mathbb{Z}_p^\times , so $l \in J$ and exists as a linear combination of n and $\phi(m)$.

Thus there is an $\bar{x} = \bar{g}^k$ such that $x^n \equiv a \pmod{m}$.

Q6

Let $p > 2$ be a prime. Prove that every primitive root of p is a quadratic nonresidue, modulo p . (HINT: Suppose a primitive root a is a residue; then every power of a is a residue.)

$$V_m = \langle a \rangle$$

but if a is a quadratic residue then

$$a^2 \equiv a \pmod{p}$$

So a cannot be a primitive root of p and a quadratic residue since it can only generate even powers of a .

Also there are $\phi(p)/2$ quadratic residues from 23H3, but $\phi(p)$ elements in V_m .

So a is not a quadratic residue.

Q7

A prime p of the form $p = 2^m + 1$ is called a Fermat prime. Let p be a Fermat prime. Prove that every quadratic nonresidue mod p is a primitive root of p .

Number of quadratic residues in \mathbb{Z}_p^\times is $(p-1)/2$ but $p = 2^m + 1$

$$\frac{p-1}{2} = \frac{(2^m + 1) - 1}{2} = 2^{m-1}$$

The number of primitive roots are the coprimes in \mathbb{Z}_p^\times which equals $\phi(\phi(p)) = \phi(p-1) = \phi((2^m + 1) - 1) = \phi(2^m)$. Since 2 is prime

$$\phi(2^m) = 2^{m-1}(2-1) = 2^{m-1}$$

From 23I6, we know every primitive root is a quadratic non-residue. Since both groups are the same size, we thus conclude that every quadratic non-residue is a primitive root.