Student: Yu Cheng (Jade)
Math 412
Worksheet #2
June 22, 2010

Worksheet #2

Question 1: How many prime factors can a 7-digit number have?

Answer: $2^{23} < 10^7 - 1 < 2^{24}$, the maximum number of prime factors is 23. The minimum number of prime factors is 2, which happens when the 7-digit number is a prime number. In this case, the only divisors are 1 and the number itself.

Question 2: Find the gcd and writ it as a line combination.

a. 33 and 71

Answer:

$$\begin{aligned} 71 &= 2 \cdot 33 + 5 \\ 33 &= 6 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} gcd &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2 \cdot (33 - 6 \cdot 5) - 5 = -13 \cdot 5 + 2 \cdot 33 \\ &= -13 \cdot (71 - 2 \cdot 33) + 2 \cdot 33 \\ &= 28 \cdot 33 - 13 \cdot 71 \end{aligned}$$

We can also take the following approach.

		2	6	1	1	2
0	1	2	13	15	28	71
1	0	1	6	7	13	33

In summary, $\gcd(33, 71) = 1$ and the linear combination is $28 \cdot 33 - 13 \cdot 71 = 1$.

b. 401 and 731

Answer:

$$\begin{aligned} 731 &= 1 \cdot 401 + 330 \\ 401 &= 1 \cdot 330 + 71 \\ 330 &= 4 \cdot 71 + 46 \\ 71 &= 1 \cdot 46 + 25 \\ 46 &= 1 \cdot 25 + 21 \end{aligned} \quad \Rightarrow \quad \begin{aligned} gcd &= 5 - 4 \\ &= (21 - 4 \cdot 4) - 4 = -5 \cdot 4 + 21 \\ &= -5 \cdot (25 - 21) + 21 = 6 \cdot 21 - 5 \cdot 25 \\ &= 6 \cdot (46 - 25) - 5 \cdot 25 = -11 \cdot 25 + 6 \cdot 46 \\ &= -11 \cdot (71 - 46) + 6 \cdot 46 = 17 \cdot 46 - 11 \cdot 71 \end{aligned}$$

$25 = 1 \cdot 21 + 4$ $= 17 \cdot (330 - 4 \cdot 71) - 11 \cdot 71 = -79 \cdot 71 + 17 \cdot 330$

$21 = 4 \cdot 4 + 5$ $= -79 \cdot (401 - 330) + 17 \cdot 330 = 96 \cdot 330 - 79 \cdot 401$

$5 = 1 \cdot 4 + 1$ $= 96 \cdot (731 - 401) - 79 \cdot 401$

$4 = 4 \cdot 1 + 0$ $= -175 \cdot 401 + 96 \cdot 731$

We can also take the following approach.

		1	1	4	1	1	1	4	1	4
0	1	1	2	9	11	20	31	144	175	844
1	0	1	1	5	6	11	17	79	96	463

In summary, $\gcd(401, 731) = 1$ and the linear combination is $96 \cdot 731 - 175 \cdot 401 = 1$.

c. 1302 and 6102

Answer:

$6102 = 4 \cdot 1302 + 894$ $gcd = 78 - 4 \cdot 18$

$1302 = 1 \cdot 894 + 408$ $= 78 - 4 \cdot (408 - 5 \cdot 78) = 21 \cdot 78 - 4 \cdot 408$

$894 = 2 \cdot 408 + 78$ $= 21 \cdot (894 - 2 \cdot 408) - 4 \cdot 408 = -46 \cdot 408 + 21 \cdot 894$

$408 = 5 \cdot 78 + 18$ $\Rightarrow$ $= -46 \cdot (1302 - 894) + 21 \cdot 894 = 67 \cdot 894 - 46 \cdot 1302$

$78 = 4 \cdot 18 + 6$ $= 67 \cdot (6102 - 4 \cdot 1302) - 46 \cdot 1302$

$18 = 3 \cdot 6 + 0$ $= 67 \cdot 6102 + (-314) \cdot 1302$

We can also take the following approach.

		4	1	2	5	4	3
0	1	4	5	14	75	314	1017
1	0	1	1	3	16	67	217

In summary, $\gcd(1302, 6102) = 6$ and the linear combination is $67 \cdot 6102 - 314 \cdot 1302 = 6$.

Question 3: Solve the following modulus arithmetic.

Answer:

a.

$5x = 1 \, mod \, 7$

$3 \times 5x = 3 \times 1 \, mod \, 7$

$15x = 3 \, mod \, 7$

$x = 3 \, mod \, 7$.

b.

$2x = 1 \, mod \, 6$

No solution.

c.

$4x = 5 \, mod \, 7$

$2 \times 4x = 2 \times 5 \, mod \, 7$

d.

$7x + 1 = 0 \, mod \, 10$

$7x = (-1) \, mod \, 10$

$8x = 10 \; mod \; 7$

$x = 3 \; mod \; 7$.

$7x = 9 \; mod \; 10$

$21x = 27 \; mod \; 10$

$x = 7 \; mod \; 10$.

e.

$3x + 4 = 2 \; mod \; 11$

$3x = -2 \; mod \; 11$

$3x = 9 \; mod \; 11$

$12x = 36 \; mod \; 11$

$x = 3 \; mod \; 11$.

f.

$x^2 = 4 \; mod \; 7$

$x = 2, 5 \; mod \; 7$.

g.

$x^2 = 2 \; mod \; 7$

$x^2 = 9 \; mod \; 7$

$x = 3, 4 \; mod \; 7$.

h.

$x^2 = 5 \; mod \; 7$

No solution.

i.

$x^2 + 1 = 0 \; mod \; 13$

$x^2 = (-1) \; mod \; 13$

$x^2 = 12 \; mod \; 13$

$x^2 = 25 \; mod \; 13$

$x = 5, 8 \; mod \; 13$.

j.

$2x = 1 \; mod \; 19$

$20x = 10 \; mod \; 19$

$x = 10 \; mod \; 19$.

k.

$2x = 1 \; mod \; 50$

No solution.

l.

$31x = 1 \; mod \; 50$

$21 \times 31x = 21 \; mod \; 50$

$651x = 21 \; mod \; 50$

$x = 21 \; mod \; 50$.

m.

$9x = 3 \; mod \; 17$

$18x = 6 \; mod \; 17$

$x = 6 \; mod \; 17$.

n.

$15x = 2 \; mod \; 35$

No solutions.

o.

$3x + 1 = 0 \; mod \; 13$

$3x = (-1) \; mod \; 13$

$(-4) \times 3x = (-4) \times 12 \; mod \; 13$

p.

$5x + 11 = 0 \; mod \; 23$

$5x = (-11) \; mod \; 23$

$5x = 12 \; mod \; 23$

$x = -48 \ mod \ 13$

$x = 4 \ mod \ 13$.

$(-9) \times 5x = (-9) \times 12 \ mod \ 23$

$-45x = -108 \ mod \ 23$

$(-45 + 2 \times 23)x = (-108 + 5 \times 23) \ mod \ 23$

$x = 7 \ mod \ 23$.

Question 4: Solve, either in $\mathbb{Z}_p$ or in a quadratic extension field.

Answer:

a.

$x^2 + 1 = 0 \ mod \ 13$

$x^2 = (-1) \ mod \ 13$

$x^2 = 12 \text{ mod } 13$

$\mathrm{x}^2 = 25 \text{ mod } 13$

$\mathrm{x} = 5, 8 \ mod \ 13$.

b.

$x^2 + 1 = 0 \ mod \ 11$

$x^2 = (-1) \ mod \ 11$

$x = i, (11 - i) \ mod \ 11$, where $i^2 = -1$.

c.

$x^2 + 2x + 7 = 0 \ mod \ 11$

$(x + 1)^2 = (-6) \ mod \ 11$

$(x + 1)^2 = 5 \ mod \ 11$

$(x + 1)^2 = 16 \ mod \ 11$

$x + 1 = 4, 7 \ mod \ 11$

$x = 3, 6 \ mod \ 11$.

d.

$x^2 + 2x + 6 = 0 \ mod \ 11$

$(x + 1)^2 = (-5) \ mod \ 11$

$(x + 1)^2 = 6 \ mod \ 11$

$(x + 1)^2 = (6 - 22) \ mod \ 11$

$(x + 1)^2 = -16 \ mod \ 11$

$x + 1 = 4i, (11 - 4i) \ mod \ 11$, where $i^2 = -1$.

e.

$x^2 + 3x + 1 = 0 \ mod \ 13$

$4x^2 + 12x + 4 = 0 \ mod \ 13$

$(2x + 3)^2 - 5 = 0 \ mod \ 13$

$(2x + 3)^2 = 5 \ mod \ 13$

No solution.

f.

$x^2 + 3x + 1 = 0 \ mod \ 13$

$4x^2 + 12x + 12 = 0 \ mod \ 13$

$(2x + 3)^2 + 3 = 0 \ mod \ 13$

$(2x + 3)^2 = (-3) \ mod \ 13$

$(2x + 3)^2 = 10 \ mod \ 13$

$(2x + 3)^2 = 49 \ mod \ 13$

$2x + 3 = 7, 6 \ mod \ 13$

$2x = 4, 3 \ mod \ 13$

$14x = 28, 21 \ mod \ 13$

$x = 2, 8 \ mod \ 13$.