#1: a) $(174, 66)$ $s = 55$ $y^2 = x^3 + 3x + 7 \bmod 199$

b)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

$0 = 15 = m$ $\quad x = 7 \cdot 15 + j = 105 + j$

j	$x = 105 + j$	$z = x^3 + 5x + 7$	$y = z^{50}$	y^2	
0	105	176	55	23	NO
1	106	140	90	140	Yes

$M_1 = (106, 90)$

$k = 11 = m$

$x = 7 \cdot 11 + j = 77 + j$

j	$x = 77 + j$	$z = x^3 + 5x + 7$	$y = z^{50}$	y^2	
0	77	21	175	178	NO
1	78	135	8	64	NO
2	79	120	26	79	NO
3	80	181	139	18	NO
4	81	125	18	125	Yes

$M_2 = (81, 18)$

#1: $y^2 = x^3 + 5x + 7 \bmod 199$ $\quad P = (1,49)$ ord 212

$Q = (174,66)$

c) $e_K(M_1) = (kP, kQ + M_1)$

$= (57(1,49),\ 57(174,66) + (106,90))$

$= ((89,168),\ (190,167) + (106,90))$

$= ((89,168),\ (60,118)) = (R,T)$

check: $d_K(R,T) = -sR + T = 101 \cdot (89,168) + (60,118)$

$= (190,32) + (60,118) = (106,90)$ ✓

$e_K(M_2) = (kP,\ kQ + M_2)$

$= ((89,168),\ (190,167) + (81,18))$

$= ((89,168),\ (88,155)) = (R,T)$

check: $d_K(R,T) = -sR + T = 101(89,168) + (88,155)$

$= (190,32) + (88,155)$

$= (81,18)$ ✓

#2 $y^2 = x^3 + 2x + 4 \bmod 31$

$P = (0,2)$ $\quad s = 11$ $\quad Q = 11 \cdot (0,2) = (10,30)$

#3: $N=15$ $P=(179,71)$ order 212

$S = K\cdot 15 + j$ $\quad Q = SP = K\cdot 15P + jP$

$Q - K15P = jP$

j	jP
0	$\mathcal{O}$
1	(179,71)
2	(198,198)
3	(53,59)
4	(18,77)
5	(190,32)
~~6~~	~~(109,115)~~
7	(55,33)
8	(195,91)
9	(38,155)
10	(61,45)
11	(178,81)
12	(141,146)
13	(1,49)

k	$K\cdot(15)P$	$+Q=(112,82)-15P = 197P = (28,127)$
0	~~(28,127)~~ $\mathcal{O}$	(112,82)
1	(28,127)	(90,91)
2	(172,41)	(130,189)
3	(164,109)	(67,60)
4	(68,89)	(66,173)
5	(184,61)	(166,83)
6	(117,102)	(185,24)
7	(84,31)	(109,115) ✓
8	(8,34)	
9	(10,96)	
10	(27,129)	
11	(148,113)	
12	(81,118)	
13	(87,102)	

so $j=6$, $K=7$

$S = 7\cdot 15 + 6 = 111$

check: $111(179,71) = (112,82)$ ✓

#4

a) $F_{16}: x^4 + x^3 + 1$

$$\begin{array}{r} 1110.1011 \\ \hline 11100 \\ 1110 \\ 1110 \\ \hline 1100010 \end{array}$$

$$\begin{array}{r|l} & 1. \\ \hline 1100010 & \\ 11001 & \\ \hline 110 & \end{array}$$

$x^3 + x.$

b) 1101^{-1} $\quad a = 1101$

$11001 = 1 \cdot m + 0 \cdot a$

$1101 = 0 \cdot m + 1 \cdot a$ (10)

$11 = 1m + 10a$ (100)

$1 = 100m + 1001a$

$a^{-1} = 1001$

check: $1001 \cdot 1101$

1001

10010

1001

1100101

$11001 \overline{)11001\,01}$ $\quad 1$

11001

1 ✓

#5: try x^2+1

$0^2+1=1$

$1^2+1=2$

$2^2+1=5\equiv 2$

} all $\neq 0$ $\Rightarrow$ irreducible

$\alpha^2 = 2$ a root

$\{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$ 9 elts

try α: $\alpha^2 = 2$, $\alpha^3 = 2\alpha$, $\alpha^4 = 2\alpha^2 = 2 \cdot 2 = 4 \equiv 1$

order 4

try $\alpha+1$: $(\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = 2 + 2\alpha + 1 = 2\alpha$

$(\alpha+1)^4 = (2\alpha)^2 = 4\alpha^2 = 1 \cdot 2 = 2 = -1$

$(\alpha+1)^8 = (-1)^2 = 1$ $\Rightarrow$ $\alpha+1$ has order 8

#6:

$$557 - 2\sqrt{557} \leq N_p \leq 557 + 2\sqrt{557}$$

($2\sqrt{557} \approx 47.2$)

$$510 \leq N_p \leq 604$$

$3 \cdot 184 = 567$ fits

567

#7:

$255 = 1 \cdot a + 0 \cdot b$ (b = 204)

$204 = 0 \cdot a + 1 \cdot b$

a = 255, b = 204

a) $51 = 1a - 1b$

#8: germany

b) 107 is prime

$177 \equiv 70$

$70^{106} = 1 \mod 107$

$70 \cdot 70^{105} = 1$

$70^{-1} = 70^{105} = 26$

check: $70 \cdot 26 = 1820 \equiv 1 \mod 107$

#9:

$x \equiv 7 \mod 8$

$x \equiv 3 \mod 9$ } 111

7, 15, 23, 31, 47, 63, 79, 95, 111

$x \equiv 23 \mod 25$

$x \equiv 111 \mod 72$

$x \equiv 39 \mod 72$

$x = 39 + k72 \equiv 23 \mod 25$

$k22 \equiv 9 \mod 25$

$22^{-1} \mod 25$?

$= 8$

$8 \cdot 22 = 176 \equiv 1 \mod 25$

$25 = 1 \cdot a + 0 \cdot b$

$22 = 0 \cdot a + 1 \cdot b$

$3 = 1a - 1 \cdot b$

$1 = -7a + 8 \cdot b$

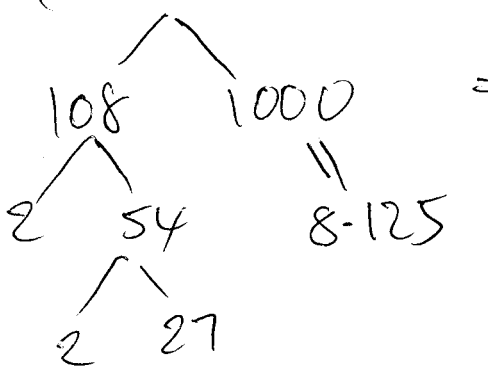
$k \equiv 8 \cdot 9 \mod 25$

$\equiv 72 \mod 25$

$\equiv 22 \mod 25$

$x = 39 + 22 \cdot 72 = 1623$

#10: a) $\phi(108000) = \phi(125)\cdot\phi(32)\,\phi(3^3)$



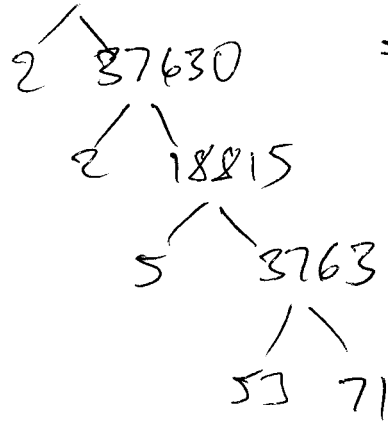
$= \phi(5^3)\,\phi(2^5)\,\phi(3^3)$

$= (125-25)(32-16)(27-9)$

$= 100 \cdot 16 \cdot 18$

$= 28{,}800$

b) $\phi(75260) = \phi(2^2)\cdot\phi(5)\cdot\phi(53)\,\phi(71)$



$= 2 \cdot 4 \cdot 52 \cdot 70$

$= 29{,}120$

#11

$587^{331} \bmod 100$

$87^{331} \equiv 63$

#12: $p = 91001$

$p-1 = 91000 = 8 \cdot 11375$

$2^{11375} = 75336$

$75336^2 = 53529$

$53529^2 = 5354$

$5354^2 \equiv 1$ Stop

$\gcd(5354^{-1}, p) = 5353$

#13 $\sqrt{31} = 5.56$ $\quad 14 \equiv 3^x$

$N = 6$ $\quad x = 6k + j$

$14 = 3^x = (3^6)^k \cdot 3^j$ $\quad 3^6 \bmod 31 \equiv 16$ $\quad \frac{1}{16} \equiv 2$

j	3^j	k	$(3^6)^k \times 16$	2^k	$2^k \cdot 14$
		0	1	1	14
0	0	1	16	2	28
1	3	2	8	4	25
2	9	3	4	8	19
3	27	4	2	16	
4	19	5	1	1	
5	26				

$j = 4 \quad k = 3$ $\quad x = 3 \cdot 6 + 4 = \underline{22}$

Check $3^{22} \equiv 14 \bmod 31$ ✓

#14

a) $78^{-1} \bmod 107$ ← prime

$78^{106} \equiv 1$

$78 \cdot 78^{105} \equiv 1$

$78^{105} \equiv 59 \bmod 107$

check: $78 \cdot 59 = 4602 \equiv 1 \pmod{107}$ ✓

b) $701^{-1} \bmod 5500 \quad = 5^3 \cdot 4 \cdot 11$

$\phi(5^3 \cdot 4 \cdot 11) =$

$\phi(5^3)\,\phi(4)\,\phi(11)$

$= 100 \cdot 2 \cdot 10 = 2000$

5 | 1100

5 | 220

5 | 44

4 | 11

$701^{2000} \equiv 1 \bmod 5500$

$701 \cdot 701^{1999} \equiv \underline{2801} \bmod 5500$

check: $701 \cdot 2801 \equiv 1 \bmod 5500$ ✓

#15:

$n = 28892177$

$2^{B!} = \left(2^{362880}\right)^{17160} = 26599275^{17160} = 15478187$

$13 \cdot 12 \cdot 11 \cdot 10 = 17160$

$9! = 362880$

$\gcd(15478186, 28892177) = \underline{6553}$