3.34

(a) If p is an odd prime, then the congruence $t^2 \equiv N \pmod{p}$ has either 0 or 2 solutions mod p.

$$t^2 \equiv N \pmod{p^e}$$

Sieve $N = 493$ up to $B = 11$ on values from $F(23)$ to $F(38)$

$F(24) = 576 - 493 = 83$
$F(25) = 625 - 493 = 132$
$F(26) = 676 - 493 = 183$
$F(27) = 729 - 493 = 236$
$F(28) = 784 - 493 = 291$
$F(29) = 841 - 493 = 348$
$F(30) = 900 - 493 = 407$

$F(31) = 961 - 493 = 468$
$F(32) = 1024 - 493 = 531$
$F(33) = 1089 - 493 = 596$
$F(34) = 1156 - 493 = 663$
$F(35) = 1225 - 493 = 732$
$F(36) = 1296 - 493 = 803$
$F(37) = 1369 - 493 = 876$
$F(38) = 1444 - 493 = 951$

36	83	132	183	236	291	348	407	468	531	596	663	732	803	876	951
↓2		↓2											↓2	↓2	↓2
18	↓3	66	91	118	×	174	×	234	×	298	×	366	×	438	
↓	×	22	×	×	97	58	×	78	177	×	221	112	×	146	317
9	×	11	×	×	×	×	×	117	×	×	×	28	×	×	×
3		1						×				14			
1												7			
												×			

$F(23) \equiv 36 \equiv 2^2 \cdot 3^2 \pmod{493}$
$F(25) \equiv 132 \equiv 2^2 \cdot 3 \cdot 11 \pmod{493}$

$\gcd(63, 493) = 17$

$\frac{493}{17} = 29$

So, $493 = 17 \cdot 29$

2. Solve $11^x \equiv 47 \bmod 103$

103 is prime, 11 is a primitive root.

(a) $g^i \pmod{103}$, 5 smooth for $i = 22, 65, 99$

$11^{22} \bmod 103 \equiv 32 \equiv 2^5$

$11^{65} \bmod 103 \equiv 20 \equiv 2^2 \cdot 5$

$11^{99} \bmod 103 \equiv 90 \equiv 2 \cdot 3^2 \cdot 5$

} 5 - smooth

$a = \log_{11}(2)$ $\quad 11^{22} \Rightarrow 2^5 \rightarrow 22 \equiv 5a \bmod 102$

$b = \log_{11}(3)$ $\quad 11^{65} \rightarrow 2^2 \cdot 5 \rightarrow 65 \equiv 2a + c \bmod 102$

$c = \log_{11}(5)$ $\quad 11^{99} \rightarrow 2 \cdot 3^2 \cdot 5 \rightarrow 99 \equiv a + 2b + c \bmod 102$

$5a \equiv 22 \bmod 102 \rightarrow a \equiv 5^{-1} \cdot 22 \bmod 102$

$a \equiv 41 \cdot 22 \bmod 102 \equiv \underline{86 = a}$

$65 \equiv 2a + c \bmod 102 \rightarrow 65 \equiv 2(84) + c \bmod 102$

$c \equiv 65 - 172 \equiv -107 \bmod 102 \rightarrow \underline{c = 97}$

$99 = a + 2b + c \rightarrow 99 \equiv 86 + 2b + c \bmod 102$

$99 \equiv 86 + 2b + 97 \bmod 102 \rightarrow b = 9$

$\log_{11}(2) \equiv 86 \bmod 102$, $\log_{11}(3) \equiv 97 \bmod 102$, $\log_{11}(5) \equiv 9 \bmod 102$

$11^x \equiv 47 \bmod 103$, $47 \cdot 11^{-97} \equiv 30 \bmod 103$

$\rightarrow x \equiv 97 + \log_{11}(30) \bmod 102$

$30 \equiv 2 \cdot 3 \cdot 5 \rightarrow \log_{11}(30) = a + b + c = 86 + 97 + 9 = 192$

$x \equiv 97 + 94 = 289$

$85 \bmod 102 = x$

3. (a) Find residue and non-residue of mod 11

$1^2 \equiv 1$
$2^2 \equiv 4$
$3^2 \equiv 9$
$4^2 \equiv 16 \equiv 5$ x
$5^2 \equiv 25 \equiv 3$ x
$6^2 \equiv 36 \equiv 3$ x
$7^2 \equiv 49 \equiv 5$ x
$8^2 \equiv 64 \equiv 9$ x
$9^2 \equiv 4$ x
$10^2 \equiv 100 \equiv 1$ x

QR : 1, 3, 4, 5, 9
NR : 2, 6, 7, 8, 10

(b) $\left(\frac{2}{11}\right) \equiv 2^{(11-1)/2} \equiv 2^5 \bmod 11$

$\equiv 10 \equiv -1 \bmod 11$

$\left(\frac{2}{11}\right) \equiv -1$ NR

(c) $\left(\frac{47}{11}\right) \rightarrow 47 \bmod 11 = \left(\frac{3}{11}\right)$

$\left(\frac{3}{11}\right) \equiv 3^{(11-1)/2} \equiv 3^5 \bmod 11 \equiv 1 \bmod 11$

$\left(\frac{3}{11}\right) \equiv 1$, $\left(\frac{47}{11}\right) = 1$ QR

4.

(a) $\left(\frac{168}{317}\right)$

1 $168 = 2^3 \cdot 3 \cdot 7$

$\left(\frac{168}{317}\right) = \left(\frac{2^3}{317}\right) \cdot \left(\frac{3}{317}\right) \cdot \left(\frac{7}{317}\right)$

$\left(\frac{2}{317}\right) : \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

$p = 317$

$\frac{317^2-1}{8} = 12561$ (odd) $\rightarrow \frac{2}{317} = -1$

$\left(\frac{3}{317}\right) = \left(\frac{317}{3}\right) \cdot (-1)^{1 \cdot 158} = \left(\frac{2}{3}\right) \cdot (-1)^{1 \cdot 158} = 1 \cdot 1 = 1$

$317 \equiv 2 \bmod 3$, $\left(\frac{2}{3}\right) = -1$

$\left(\frac{7}{317}\right)$, 7 is QR, so $= 1$

$\left(\frac{168}{317}\right) = -1 \cdot -1 \cdot 1 = 1$

(b) Since $\left(\frac{168}{317}\right) = 1$, this means 168 IS A QUADRATIC RESIDUE mod 317

5.

$\left(\frac{53}{113}\right)$

$\left(\frac{53}{113}\right) = \left(\frac{113}{53}\right) = \left(\frac{7}{53}\right) = \left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = 1$

$53 \bmod 7 = 4$

4 is A perfect square

$53 \equiv 1 \bmod 4$
$113 \equiv 1 \bmod 4$

$113 \bmod 53 = 7$

$53 \bmod 4 = 1$
$7 \bmod 4 = 3$

So, $\left(\frac{53}{113}\right) = 1$