Then, clearly, $\gcd(x,m)=1$,
so that $x = g^k$ for some

$$k \in \{0,1,2,\dots,\phi(m)-1\}.$$

Then the congruence $x^2 \equiv 1 \pmod m$
is equivalent to the congruence

$$g^{2k} \equiv 1 = g^0 \pmod{m},$$

which gives the congruence

$$2k \equiv 0 \pmod{\phi(m)}.$$

Since $m>2 \Rightarrow \phi(m)$ is even.
Dividing by 2:

$$k \equiv 0 \left(\bmod \frac{\phi(m)}{2}\right),$$

whence $k = s \cdot \frac{\phi(m)}{2}$, $s \in \mathbb{Z}$

If $s = 2t$ for some $t \in \mathbb{Z}$,
then $k = s \cdot \frac{\phi(m)}{2} = 2t \frac{\phi(m)}{2} = 2\phi(m)$

$\Rightarrow k \equiv 0 \pmod{\phi(m)}$
If $s = 2t+1$ for some $t \in \mathbb{Z}$,
then

$$k = (2t+1)\frac{\phi(m)}{2} = t\phi(m) + \frac{\phi(m)}{2},$$

whence $k \equiv \frac{\phi(m)}{2} \pmod{\phi(m)}$.

and, moreover, $k \in \{0, 1, 2, \ldots, \phi(m)-1\}$.

This gives two solutions

$g^0 = 1$ and $g^{\frac{\phi(m)}{2}}$ mod m.

BW (iii) Since $m = 3p^s$, $s > 0$ and $p \neq 3$, $\gcd(3, p^s) = 1$

and $a^{\frac{1}{2}\phi(m)} \equiv 1 \pmod m$

by (i). Then $|a|_m \mid \left(\frac{1}{2}\phi(m)\right) \Rightarrow$

$\Rightarrow |a|_m \leq \frac{1}{2}\phi(m) < \phi(m) \Rightarrow$

$\Rightarrow$ any $a \in \mathbb{Z}$, such that $\gcd(a, m) = 1$, can <u>not</u> be a primitive root.

(iv)

BW
HW

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^s	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

$$|3|_{17} = 16 = \phi(17)$$

3 – prim. root

$$5 = 3^5 \quad \& \quad 11 = 3^7$$

$$5^x \equiv 11 \pmod{17} \iff (3^5)^x \equiv 3^7 \pmod{17}$$

$$\iff 5x \equiv 7 \pmod{16}$$

$$\gcd(5, 16) = 1$$

$$1 \cdot 16 + (-3) \cdot 5 = 16 - 15 = 1$$

$$(-3) \cdot 5 \equiv 1 \pmod{16}$$

$$x \equiv (-3) \cdot 5x \equiv (-3)\, 7 \pmod{16}$$

$$x \equiv -21 \pmod{16} \equiv -5 \equiv 11 \pmod{16}$$

$$x \equiv 11 \pmod{16}$$

Problem 7:

BW HW (i) Let p be a prime, and let $n \in \mathbb{Z}$ such that $\gcd(n,p)=1$. Then n is called a quadratic residue modulo m if $\exists\, a \in \mathbb{Z}$, such that

$$n \equiv a^2 \pmod{m}.$$

Legendre Symbol:

$$\left(\frac{n}{p}\right) = \begin{cases} +1, & \text{if } n \text{ is a quadratic residue} \\ -1, & \text{if } n \text{ is not a quadratic residue} \end{cases}$$

(ii) BW Euler's Criterion in the first form:
Let p be a prime, $p>2$, and let g be a primitive root mod p. Let n be a positive integer coprime to p.
Then:

if $n \equiv g^k \pmod{p}$ then

k is even $\Leftrightarrow n^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow$

$\Leftrightarrow n \equiv m^2 \pmod{p}$ for some $m \Leftrightarrow$

$\Leftrightarrow \left(\frac{n}{p}\right) = +1$

k is odd $\Leftrightarrow n^{\frac{p-1}{2}} \equiv -1 \pmod{p} \Leftrightarrow$

$\Leftrightarrow n \not\equiv m^2 \pmod{p}$ for all $m \in \mathbb{Z} \Leftrightarrow$

$\Leftrightarrow \left(\frac{n}{p}\right) = -1$

Euler's criterion in the second form:

Let n be a positive integer and let p be a prime, $\gcd(n,p)=1$.

Then

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p .$$

In particular,

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

Also:

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8 \\ -1, & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

(iii) By Euler's Criterion:

BW

MW

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \quad \& \quad \left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \quad \&$$

$$\left(\frac{mn}{p}\right) = (mn)^{\frac{p-1}{2}} .$$ Then:

$$\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} = (mn)^{\frac{p-1}{2}} = \left(\frac{mn}{p}\right)$$

Moreover, since for two $n, n' \in \mathbb{Z}$, such that $n \equiv n' \pmod p$, n is a quadratic residue mod p if and only if so is n', we get

$$\left(\frac{n}{p}\right) = \left(\frac{n+kp}{p}\right) \text{ for } \forall k \in \mathbb{Z}, \text{ i.e.}$$

$$\left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right) \text{ provided } n \equiv n' \pmod p .$$

BW
HW

(v) $\left(\frac{77}{67}\right) = \left(\frac{7\cdot 11}{67}\right) = \left(\frac{7}{67}\right)\left(\frac{11}{67}\right)$ (25)

$$\left(\frac{7}{67}\right)\left(\frac{67}{7}\right) = (-1)^{\frac{(7-1)(67-1)}{4}} = (-1)^{3\cdot 33} = -1 \Rightarrow$$

$$\Rightarrow \left(\frac{7}{67}\right) = -\left(\frac{67}{7}\right) = -\left(\frac{63+4}{7}\right) = -\left(\frac{4}{7}\right) =$$

$$= -\left(\frac{2}{7}\right)^2 = -1$$

$$\left(\frac{11}{67}\right)\left(\frac{67}{11}\right) = (-1)^{\frac{10\cdot 66}{4}} = (-1)^{5\cdot 33} = -1$$

$$\left(\frac{11}{67}\right) = -\left(\frac{67}{11}\right) = -\left(\frac{66+1}{11}\right) = -\left(\frac{1}{11}\right) = -1$$

Then $\left(\frac{77}{67}\right) = \left(\frac{7}{67}\right)\left(\frac{11}{67}\right) = (-1)(-1) = +1$

$$\left(\frac{124}{103}\right) = \left(\frac{4\cdot 31}{103}\right) = \left(\frac{2}{103}\right)^2 \left(\frac{31}{103}\right) = \left(\frac{31}{103}\right)$$

$$\left(\frac{31}{103}\right)\left(\frac{103}{31}\right) = (-1)^{\frac{30\cdot 102}{4}} = (-1)^{15\cdot 51} = -1$$

$$\left(\frac{31}{103}\right) = -\left(\frac{103}{31}\right) = -\left(\frac{93+10}{31}\right) = -\left(\frac{10}{31}\right) =$$

$$= -\left(\frac{2\cdot 5}{31}\right) = -\left(\frac{2}{31}\right)\left(\frac{5}{31}\right) = -\left(\frac{5}{31}\right)$$

because $31 \equiv -1 \pmod 8$.

$$\left(\frac{5}{31}\right)\left(\frac{31}{5}\right) = (-1)^{\frac{4\cdot 30}{4}} = (-1)^{30} = +1 \Rightarrow$$

$\left(\frac{5}{31}\right) = \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = +1$, so that

$$\left(\frac{124}{103}\right) = \left(\frac{31}{103}\right) = -\left(\frac{5}{31}\right) = -1$$

$$\left(\frac{176}{211}\right) = \left(\frac{2^4 . 11}{211}\right) = \left(\frac{11}{211}\right)$$

$$\left(\frac{11}{211}\right)\left(\frac{211}{11}\right) = (-1)^{\frac{10 . 210}{4}} = (-1)^{5 . 105} = -1$$

$$\left(\frac{11}{211}\right) = -\left(\frac{211}{11}\right) = -\left(\frac{19 . 11 + 2}{11}\right) = -\left(\frac{2}{11}\right) = +1$$

as $11 \equiv 3 \pmod 8$. Then

$$\left(\frac{176}{211}\right) = \left(\frac{11}{211}\right) = +1$$