Solve $x^2 \equiv 5 \pmod{1601}$ ($7 =$ primitive root)

$$
\begin{aligned}
x &\equiv 7^k \pmod{1601} \\
5 &\equiv 7^{\ell} \pmod{1601} \\
x^2 &\equiv 5 \pmod{1601} \\
7^{2k} &\equiv 7^{\ell} \pmod{1601}
\end{aligned}
$$

Solve $x^2 \equiv 5 \pmod{1601}$ ($7 =$ primitive root)

$$
\begin{aligned}
x &\equiv 7^k \pmod{1601} \\
5 &\equiv 7^{\ell} \pmod{1601} \\
x^2 &\equiv 5 \pmod{1601} \\
7^{2k} &\equiv 7^{\ell} \pmod{1601}
\end{aligned}
$$

$$
\begin{aligned}
2k &\equiv \ell \pmod{1600} \\
2k &\equiv \ell \pmod{64} \\
2k &\equiv \ell \pmod{25}
\end{aligned}
$$

Solve for $k \pmod{1600}$

$$
\begin{aligned}
2k &\equiv \ell \pmod{25} \\
k &\equiv 2^{-1}\ell \pmod{25} \\
k &\equiv 13\ell \pmod{25} \\
k &\equiv ?? \pmod{1600}
\end{aligned}
$$

Solve for $k \pmod{1600}$

$$
\begin{aligned}
2k &\equiv \ell \pmod{25} \\
k &\equiv 2^{-1}\ell \pmod{25} \\
k &\equiv 13\ell \pmod{25} \\
k &\equiv ?? \pmod{1600} \\
k &\equiv 13\ell + 25N \pmod{1600}.
\end{aligned}
$$

With $N = 0, 1, \ldots, ?$.

Solve for $k \pmod{1600}$

$$
\begin{aligned}
2k &\equiv \ell \pmod{25} \\
k &\equiv 2^{-1}\ell \pmod{25} \\
k &\equiv 13\ell \pmod{25} \\
k &\equiv ?? \pmod{1600} \\
k &\equiv 13\ell + 25N \pmod{1600}.
\end{aligned}
$$

With $N = 0, 1, \ldots, ?$.

$$N = 0, 1, \ldots, 63.$$

What is x? Is it a solution to $x^2 \equiv 5 \pmod{1601}$?

Testing phase: Does this work?

$$x \equiv 7^k \equiv 7^{13\ell+25N} \pmod{1601}$$

$$x \equiv 7^k \equiv (\underbrace{7^{\ell}}_{5})^{13} \cdot (7^{25})^N \pmod{1601}$$

How to check?

What is x? Is it a solution to $x^2 \equiv 5 \pmod{1601}$?

Testing phase: Does this work?

$$x \equiv 7^k \equiv 7^{13\ell+25N} \pmod{1601}$$

$$x \equiv 7^k \equiv (\underbrace{7^{\ell}}_{5})^{13} \cdot (7^{25})^N \pmod{1601}$$

How to check?

$$5 \stackrel{?}{\equiv} x^2 \equiv 5^{26} \cdot (7^{50})^N \pmod{1601}.$$

$$5 \stackrel{?}{\equiv} 1433 \cdot 206^N \pmod{1601}.$$

Is $1433 \cdot 206^N \equiv 5 \pmod{1601}$?

N goes from 0 to 63 row by row in the table:

1433	614	5	1030	848	179	51	900
1285	545	200	1175	299	756	439	778
168	987	1596	571	753	1422	1550	701
316	1056	1401	426	1302	845	1162	823
1433	614	5	1030	848	179	51	900
1285	545	200	1175	299	756	439	778
168	987	1596	571	753	1422	1550	701
316	1056	1401	426	1302	845	1162	823

Is $1433 \cdot 206^N \equiv 5 \pmod{1601}$?

N goes from 0 to 63 row by row in the table:

1433	614	5	1030	848	179	51	900
1285	545	200	1175	299	756	439	778
168	987	1596	571	753	1422	1550	701
316	1056	1401	426	1302	845	1162	823
1433	614	5	1030	848	179	51	900
1285	545	200	1175	299	756	439	778
168	987	1596	571	753	1422	1550	701
316	1056	1401	426	1302	845	1162	823

$\boxed{N = 2, 34.}$

This is repulsive to check!

Idea: $7^{800} \equiv -1 \pmod{1601}$

We need to check

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{50})^N \pmod{1601}.$$

What do we know about exponents of $7 \pmod{1601}$?

$$7^{1600} \equiv 1 \pmod{1601}$$
$$7^{800} \equiv -1 \pmod{1601}.$$

Any ideas how to use these?

Idea: $7^{800} \equiv -1 \pmod{1601}$

We need to check

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{50})^N \pmod{1601}.$$

What do we know about exponents of $7 \pmod{1601}$?

$$7^{1600} \equiv 1 \pmod{1601}$$
$$7^{800} \equiv -1 \pmod{1601}.$$

Any ideas how to use these? Raise to the 16th power!

$$\underbrace{5^{16}}_{361} \stackrel{?}{\equiv} 5^{26 \cdot 16} \cdot (7^{800})^N \equiv \underbrace{5^{26 \cdot 16}}_{361} \cdot (-1)^N \pmod{1601}.$$

Idea: $7^{800} \equiv -1 \pmod{1601}$

We need to check

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{50})^N \pmod{1601}.$$

What do we know about exponents of $7 \pmod{1601}$?

$$7^{1600} \equiv 1 \pmod{1601}$$
$$7^{800} \equiv -1 \pmod{1601}.$$

Any ideas how to use these? Raise to the 16th power!

$$\underbrace{5^{16}}_{361} \stackrel{?}{\equiv} 5^{26 \cdot 16} \cdot (7^{800})^N \equiv \underbrace{5^{26 \cdot 16}}_{361} \cdot (-1)^N \pmod{1601}.$$

$\boxed{N = 2N_1 \text{ with } N_1 = 0, 1, \ldots, 31.}$

$N = 2N_1,\ N_1 = 0, 1, \ldots, 31$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{100})^{N_1} \pmod{1601}$$

$N = 2N_1,\ N_1 = 0, 1, \ldots, 31$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{100})^{N_1} \pmod{1601}$$

$$\underbrace{5^8}_{-19} \stackrel{?}{\equiv} 5^{26\cdot 8} \cdot (7^{800})^{N_1} \equiv \underbrace{5^{26\cdot 8}}_{19} \cdot (-1)^{N_1} \pmod{1601},$$

$N = 2N_1,\ N_1 = 0, 1, \ldots, 31$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{100})^{N_1} \pmod{1601}$$

$$\underbrace{5^8}_{-19} \stackrel{?}{\equiv} 5^{26\cdot 8} \cdot (7^{800})^{N_1} \equiv \underbrace{5^{26\cdot 8}}_{19} \cdot (-1)^{N_1} \pmod{1601},$$

$$\boxed{N_1 = 2N_2 + 1,\ N_2 = 0, 1, \ldots, 15.}$$

$N = 2N_1,\ N_1 = 0, 1, \ldots, 31$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{100})^{N_1} \pmod{1601}$$

$$\underbrace{5^8}_{-19} \stackrel{?}{\equiv} 5^{26\cdot 8} \cdot (7^{800})^{N_1} \equiv \underbrace{5^{26\cdot 8}}_{19} \cdot (-1)^{N_1} \pmod{1601},$$

$$\boxed{N_1 = 2N_2 + 1,\ N_2 = 0, 1, \ldots, 15.}$$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{100})^{2N_2+1} \equiv 5^{26} \cdot 7^{100} \cdot (7^{200})^{N_2} \pmod{1601}$$

$N = 2N_1,\ N_1 = 0, 1, \ldots, 31$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{100})^{N_1} \pmod{1601}$$

$$\underbrace{5^8}_{-19} \stackrel{?}{\equiv} 5^{26\cdot 8} \cdot (7^{800})^{N_1} \equiv \underbrace{5^{26\cdot 8}}_{19} \cdot (-1)^{N_1} \pmod{1601},$$

$$\boxed{N_1 = 2N_2 + 1,\ N_2 = 0, 1, \ldots, 15.}$$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot (7^{100})^{2N_2+1} \equiv 5^{26} \cdot 7^{100} \cdot (7^{200})^{N_2} \pmod{1601}$$

$$\underbrace{5^4}_{625} \equiv 5^{26\cdot 4} \cdot 7^{400} \cdot (7^{200})^{N_2} \equiv \underbrace{5^{26\cdot 4} \cdot 7^{400}}_{625} \cdot (-1)^{N_2} \pmod{1601},$$

$$\boxed{N_2 = 2N_3,\ N_3 = 0, 1, \ldots, 7.}$$

$$N = 2N_1,\ N_1 = 2N_2 + 1,\ N_2 = 2N_3$$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot 7^{100} \cdot (7^{400})^{N_3} \pmod{1601}$$

$$N = 2N_1,\ N_1 = 2N_2 + 1,\ N_2 = 2N_3$$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot 7^{100} \cdot (7^{400})^{N_3} \pmod{1601}$$

$$\underbrace{5^2}_{25} \equiv \underbrace{5^{26\cdot 2} \cdot 7^{200}}_{25} \cdot (-1)^{N_3} \pmod{1601}$$

$$\boxed{N_3 = 2N_4,\ N_4 = 0, 1, 2, 3.}$$

$$N = 2N_1,\ N_1 = 2N_2 + 1,\ N_2 = 2N_3$$

$$5 \stackrel{?}{\equiv} 5^{26} \cdot 7^{100} \cdot (7^{400})^{N_3} \pmod{1601}$$

$$\underbrace{5^2}_{25} \equiv \underbrace{5^{26\cdot 2} \cdot 7^{200}}_{25} \cdot (-1)^{N_3} \pmod{1601}$$

$$\boxed{N_3 = 2N_4,\ N_4 = 0, 1, 2, 3.}$$

$$5 \stackrel{?}{\equiv} \underbrace{5^{26} \cdot 7^{100}}_{5} \cdot (-1)^{N_4} \pmod{1601}$$

$$\boxed{N_4 = 0 \text{ or } 2.}$$

$$N = 2N_1,\ N_1 = 2N_2 + 1,\ N_2 = 2N_3,\ N_3 = 2N_4$$

$$N = 2N_1,\ N_1 = 2N_2 + 1,\ N_2 = 2N_3,\ N_3 = 2N_4$$

$$N_4 = 0, 2$$
$$N_3 = 0, 4$$
$$N_2 = 0, 8$$
$$N_1 = 1, 17$$
$$N = 2, 34$$

$$N = 2N_1,\ N_1 = 2N_2 + 1,\ N_2 = 2N_3,\ N_3 = 2N_4$$

$$\begin{aligned}
N_4 &= 0, 2 \\
N_3 &= 0, 4 \\
N_2 &= 0, 8 \\
N_1 &= 1, 17 \\
N &= 2, 34 \\
x &\equiv 5^{13} \cdot (7^{50})^N \\
&\equiv 1463 \cdot 1426^N \pmod{1601} \\
x &\equiv \boxed{390, 1211 \pmod{1601}}.
\end{aligned}$$