More *Repeated Squaring* Examples

Version of March 16, 2010

Evaluate $2^{50} \bmod 19$.

This can be solved by repeated squaring. Set $I_i = 2^{2^i} \bmod 19$.

$$
\begin{array}{lcllll}
I_0 & = & 2^1 \bmod 19 & & & = 2 \\
I_1 & = & 2^2 \bmod 19 & = & I_0 \cdot I_0 \bmod 19 & = 4 \\
I_2 & = & 2^4 \bmod 19 & = & I_1 \cdot I_1 \bmod 19 & = 16 \\
I_3 & = & 2^8 \bmod 19 & = & I_2 \cdot I_2 \bmod 19 & = 9 \\
I_4 & = & 2^{16} \bmod 19 & = & I_3 \cdot I_3 \bmod 19 & = 5 \\
I_5 & = & 2^{32} \bmod 19 & = & I_4 \cdot I_4 \bmod 19 & = 6
\end{array}
$$

Evaluate $2^{50} \bmod 19$.

This can be solved by repeated squaring. Set $I_i = 2^{2^i} \bmod 19$.

$$
\begin{array}{lcllll}
I_0 & = & 2^1 \bmod 19 & & & = 2 \\
I_1 & = & 2^2 \bmod 19 & = & I_0 \cdot I_0 \bmod 19 & = 4 \\
I_2 & = & 2^4 \bmod 19 & = & I_1 \cdot I_1 \bmod 19 & = 16 \\
I_3 & = & 2^8 \bmod 19 & = & I_2 \cdot I_2 \bmod 19 & = 9 \\
I_4 & = & 2^{16} \bmod 19 & = & I_3 \cdot I_3 \bmod 19 & = 5 \\
I_5 & = & 2^{32} \bmod 19 & = & I_4 \cdot I_4 \bmod 19 & = 6
\end{array}
$$

$$2^{50} = 2^{32} \cdot 2^{16} \cdot 2^2 \quad \rightarrow$$

$$
\begin{aligned}
2^{50} \bmod 19 &= I_5 \cdot I_4 \cdot I_1 \bmod 19 \\
&= 6 \cdot 5 \cdot 4 \bmod 19 \\
&= 6
\end{aligned}
$$

Evaluate $2^{41} \bmod 19$.

This can be solved by repeated squaring. Set $I_i = 2^{2^i} \bmod 19$.

$$
\begin{array}{lcllll}
I_0 & = & 2^1 \bmod 19 & & & = \quad 2 \\
I_1 & = & 2^2 \bmod 19 & = & I_0 \cdot I_0 \bmod 19 & = \quad 4 \\
I_2 & = & 2^4 \bmod 19 & = & I_1 \cdot I_1 \bmod 19 & = \quad 16 \\
I_3 & = & 2^8 \bmod 19 & = & I_2 \cdot I_2 \bmod 19 & = \quad 9 \\
I_4 & = & 2^{16} \bmod 19 & = & I_3 \cdot I_3 \bmod 19 & = \quad 5 \\
I_5 & = & 2^{32} \bmod 19 & = & I_4 \cdot I_4 \bmod 19 & = \quad 6
\end{array}
$$

Evaluate $2^{41} \bmod 19$.

This can be solved by repeated squaring. Set $I_i = 2^{2^i} \bmod 19$.

$$
\begin{array}{lllllll}
I_0 & = & 2^1 \bmod 19 & & & = & 2 \\
I_1 & = & 2^2 \bmod 19 & = & I_0 \cdot I_0 \bmod 19 & = & 4 \\
I_2 & = & 2^4 \bmod 19 & = & I_1 \cdot I_1 \bmod 19 & = & 16 \\
I_3 & = & 2^8 \bmod 19 & = & I_2 \cdot I_2 \bmod 19 & = & 9 \\
I_4 & = & 2^{16} \bmod 19 & = & I_3 \cdot I_3 \bmod 19 & = & 5 \\
I_5 & = & 2^{32} \bmod 19 & = & I_4 \cdot I_4 \bmod 19 & = & 6
\end{array}
$$

$$2^{41} = 2^{32} \cdot 2^8 \cdot 2^1 \quad \rightarrow$$

$$
\begin{aligned}
2^{41} \bmod 19 &= I_5 \cdot I_3 \cdot I_0 \bmod 19 \\
&= 6 \cdot 9 \cdot 2 \bmod 19 \\
&= 13
\end{aligned}
$$

Evaluate $3^{50} \bmod 19$.

This can be solved by repeated squaring. Set $I_i = 3^{2^i} \bmod 19$.

$$
\begin{array}{lcllcl}
I_0 & = & 3^1 \bmod 19 & & = & 3 \\
I_1 & = & 3^2 \bmod 19 & = I_0 \cdot I_0 \bmod 19 & = & 9 \\
I_2 & = & 3^4 \bmod 19 & = I_1 \cdot I_1 \bmod 19 & = & 5 \\
I_3 & = & 3^8 \bmod 19 & = I_2 \cdot I_2 \bmod 19 & = & 6 \\
I_4 & = & 3^{16} \bmod 19 & = I_3 \cdot I_3 \bmod 19 & = & 17 \\
I_5 & = & 3^{32} \bmod 19 & = I_4 \cdot I_4 \bmod 19 & = & 4
\end{array}
$$

Evaluate $3^{50} \bmod 19$.

This can be solved by repeated squaring. Set $I_i = 3^{2^i} \bmod 19$.

$$
\begin{array}{lcllll}
I_0 & = & 3^1 \bmod 19 & & & = 3 \\
I_1 & = & 3^2 \bmod 19 & = & I_0 \cdot I_0 \bmod 19 & = 9 \\
I_2 & = & 3^4 \bmod 19 & = & I_1 \cdot I_1 \bmod 19 & = 5 \\
I_3 & = & 3^8 \bmod 19 & = & I_2 \cdot I_2 \bmod 19 & = 6 \\
I_4 & = & 3^{16} \bmod 19 & = & I_3 \cdot I_3 \bmod 19 & = 17 \\
I_5 & = & 3^{32} \bmod 19 & = & I_4 \cdot I_4 \bmod 19 & = 4
\end{array}
$$

$3^{50} = 3^{32} \cdot 3^{16} \cdot 3^2$ 

$$
\begin{aligned}
3^{50} \bmod 19 &= I_5 \cdot I_4 \cdot I_1 \bmod 19 \\
&= 4 \cdot 17 \cdot 9 \bmod 19 \\
&= 4
\end{aligned}
$$