47] As $p-1 \equiv -1 \pmod p$ and $-1^2 \equiv 1$ we have Order Mod$_p(p-1) = 2$. By the order formula there is $\varphi(\varphi(2)) = 1$ element of order 2 namely $g^{\frac{p-1}{2}}$.

49] If there are small prime divisors, Pohlig-Hellman and Wiener-Lipton can be used to reduce the discrete log calculation. So p_1 is easiest, p_2 is hardest (as $p-1$ involves the largest prime factor)

51] $A \bmod 2 \equiv \begin{pmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&1 \end{pmatrix}$, so clearly $\det(A) \equiv 0 \pmod 2$

$A \bmod 5 \equiv \begin{pmatrix} 1&0&0&0 \\ 4&2&1&0 \\ 3&0&3&2 \\ 2&3&3&2 \end{pmatrix}$ subtract ↻ swap, clearly skip.

$\rightsquigarrow \begin{pmatrix} 1&0&0&0 \\ 1&2&0&0 \\ 4&2&1&0 \\ 2&3&3&2 \end{pmatrix}$, so $\det(A) \equiv -2 \cdot 2 \equiv 1 \pmod 5$

Solve with CRT: $\left.\begin{matrix} d \equiv 0 (2) \\ d \equiv 1 (5) \end{matrix}\right) \Rightarrow d = 0 + y \cdot 2 \overset{!}{\equiv} 1 \pmod 5$

Use: $2^{-1} \equiv 3 \pmod 5$ get $y = 3$

$\Rightarrow d = 2 \cdot 3 = 6$

52) Let $n = \prod p_i^{e_i}$ $\Rightarrow \varphi(n) = \prod (p_i - 1)\, p_i^{e_i - 1}$

For $\varphi(n) = 2$ all factors in this product can be of 1 or 2. Thus:

- Maximum $p_i > 3$ (otherwise $(p_i - 1) \geq 4$)
- 3^{e_i} can only be $3^0, 3^1$ (otherwise $3^{e_i - 1} \geq 3$)
- 2^{e_i} can only be $2^0, 2^1, 2^2$ (otherwise $2^{e_i - 1} \geq 4$)

$\Rightarrow$ Candidates for n must divide $2^2 \cdot 3 = 12$

Test which $n = 2, 3, 4, 6$ are the only ones with

These are those n s.t. $\sin(\pi/n)$, $\cos(\pi/n)$ are given for memorization

(the only n s.t. $\sin\left(\frac{\pi}{n}\right)$ is at most a square root)

50) If n is the time to all events on same day then

$n \equiv -2 \equiv 5 \pmod{17} \Rightarrow c_0 = 5$

$n \equiv -7 \equiv 5 \pmod{12} \Rightarrow c_1 = 5$ (lucky coincidence)

$n \equiv -1 \equiv 94 \pmod{95} \Rightarrow n = 5 + y \cdot (7 \cdot 12)$

$= 5 + y \cdot 84 \overset{!}{\equiv} 94 \pmod{95}$

$\Rightarrow y \cdot 84 \equiv 89 \pmod{95}$.

Calculate $84^{-1} \bmod 95$:

$95 = 1 \cdot 84 + 11$

$84 = 7 \cdot 11 + 7$

$11 = 7 + 4$

$7 = 4 + 3$

$4 = 3 + 1$

$\Rightarrow 1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (11 - 7) - 7$

$= 2 \cdot 11 - 3 \cdot 7 = 2 \cdot 11 - 3 \cdot (84 - 7 \cdot 11) = 23 \cdot 11 - 3 \cdot 84$

$= 23 \cdot (95 - 84) - 3 \cdot 84 = 23 \cdot 95 - 26 \cdot 84$

$\Rightarrow 84^{-1} \equiv 26 \pmod{95} \Rightarrow y \equiv 89 \cdot 26 = 2314 \equiv 34 \pmod{95}$

$\Rightarrow y = 5 + 84 \cdot 34 = \underline{\underline{2861}}$ days.

48| $a = 9,\ b = 597$. Find, s.t. $a^e \equiv b \pmod p$

Let $e = e_0 + 3e_1 + 9e_2 + 27e_3$.

Then $a^{27} \equiv 365 \pmod p$, $b^{27} \equiv 365 \pmod p$

$\Rightarrow e_0 = 1$.

Consider $b/a^{e_0} \equiv 931$, (must be power of a^3)

$931^9 \equiv 1 \pmod p$, i.e. $931^9 \equiv (a^9)^0 \Rightarrow e_1 = 0$

$931/a^{0.3} \equiv 931$.

$931^3 \equiv 1 \pmod p \Rightarrow e_2 = 0$, $931/a^{0.9} \equiv 931$

Now with $931^1 \equiv 931$ as power of $a^{27} \equiv 365$.

Exponent is $e_3 = 2$. (Can also be $0, 1, 2$; and 0 and 1 are easily recognized). Thus

$$e = 1 + 2 \cdot 27 = 55$$