① Fermat: $n^p \equiv n \mod p$

Reduce $n + n^3 + n^5 \mod 3$:

$$n + n^3 + n^3 n^2 \equiv n + n + n n^2$$

$$= n + n + n^3 \equiv n + n + n \equiv 3n \equiv 0 \mod 3$$

☺

<u>Alt</u>: In $\mathbb{Z}_3$ $n = 0, 1, 2$

If $n = 0$, we get 0

If $n = 1$, $1 + 1 + 1 = 3 \equiv 0$

If $n \equiv -1$, $-1 - 1 - 1 = -3 \equiv 0$ ☺

② $\gcd(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \mod m$

(Gen. Fermat (Euler))

$ed \equiv 1 \mod \phi(m) \Rightarrow$

$ed = 1 + k\,\phi(m)$ for some k

$$(a^e)^d = a^{ed} = a^{1 + k\phi(m)} = a \cdot \left(a^{\phi(m)}\right)^k$$

$$\equiv a \cdot 1^k \equiv a \mod m$$ ☺

<u>Note</u>: This is how RSA works! ☺

(3) Take powers of 11 mod 45:

$\langle 11 \rangle = \{11, 31, 26, 16, 41, 1\}$

Note: $|11| = 6$, $|U(45)| = \phi(5 \cdot 3^2) = 4 \cdot 6 = 24$

$\therefore$ By Lagrange's theorem the index is $\frac{24}{6} = 4$

$2\langle 11 \rangle = \{22, 17, 7, 32, 37, 2\}$

$4\langle 11 \rangle = \{44, 34, 14, 19, 29, 4\}$

$8\langle 11 \rangle = \{43, 23, 28, 38, 13, 8\}$

In the factor group $U(45)/\langle 11 \rangle$ order of the trivial coset $\langle 11 \rangle$ is 1.

Powers of 2: 4, 8, 16 $\quad \therefore |2\langle 11 \rangle| = 4$

4: 16 $\quad \therefore |4\langle 11 \rangle| = 2$

8: 19, 17, 1 $\quad \therefore |8\langle 11 \rangle| = 4$

(4)

$$\left.\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 1 \bmod 4 \\ x &\equiv 3 \bmod 5 \end{aligned}\right\}$$ pairwise co-prime ☺

$m = 3 \cdot 4 \cdot 5 = 60$

m_i	$M_i = m/m_i$	$M_i \bmod m_i$	$M_i^{-1} \bmod m_i$	r.h.s.
3	20	2	2	2
4	15	3	3	1
5	12	2	3	3

$x \equiv 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 3 = 233 \equiv 53 \bmod 60$

Check: $53 \bmod 3 = 2$

$53 \bmod 4 = 1$

$53 \bmod 5 = 3$ ☺

File Edit Cell Maxima Equations Algebra Calculus Simplify Plot Numeric Help

```
Take powers of 11 mod 45 to get <11>.  Multiply by k's to get cosets.

(%i1) cosets:create_list(create_list(mod(k*11^i,45),i,1,6),k,[1,2,4,8]);
(%o1) [[11,31,26,16,41,1],[22,17,7,32,37,2],[44,34,14,19,29,4],[43,23,28,38,
13,8]]

Take powers of cosets and see which power gets you back inside <11>

(%i2) create_list(create_list(mod(cosets[k]^i,45),i,1,4),k,1,4);
(%o2) [[[11,31,26,16,41,1],[31,16,1,31,16,1],[26,1,26,1,26,1],[16,31,1,16,31
,1]],[[22,17,7,32,37,2],[34,19,4,34,19,4],[28,8,28,8,28,8],[31,1,16,31,1,16]
],[[44,34,14,19,29,4],[1,31,16,1,31,16],[44,19,44,19,44,19],[1,16,31,1,16,31]
],[[43,23,28,38,13,8],[4,34,19,4,34,19],[37,17,37,17,37,17],[16,31,1,16,31,1]
]]
```

Welcome to wxMaxima

Ready for user input

File Edit Cell Maxima Equations Algebra Calculus Simplify Plot Numeric Help

```
(%i1) rems:[2,1,3];
      mods:[3,4,5];
(%o1) [2,1,3]
(%o2) [3,4,5]

(%i3) m:product(mods[i],i,1,3);
(%o3) 60

(%i4) M:create_list(m/mods[i],i,1,3);
(%o4) [20,15,12]

(%i5) create_list(mod(M[i],mods[i]),i,1,3);
      Mi:create_list(inv_mod(%[i],mods[i]),i,1,3);
(%o5) [2,3,2]
(%o6) [2,3,3]

(%i7) sum(M[i]*Mi[i]*rems[i],i,1,3); mod(%,m);
(%o7) 233
(%o8) 53
```

Check the answer

```
(%i9) x:chinese(rems,mods);
      mod(x,mods);
      %-rems;
(%o9) 53
(%o10) [2,1,3]
(%o11) [0,0,0]
```

Welcome to wxMaxima Ready for user input