1. $342 = 181 + 161$ $\quad$ $1 = 160 - 8\cdot 20 = 160 - 8(181 - 161) =$

$181 = 161 + 20$ $\quad$ $= -8\cdot 181 + 9\cdot 161 = -8\cdot 181 + 9(342 - 181)$

$160 = 8\cdot 20 + 1$ $\quad$ $= 9\cdot 342 - 17\cdot 181$

$\underbrace{1}_{\text{gcd}}$ $\quad$ $\underbrace{9}_{s}$, $\underbrace{-17}_{t}$

2. Suppose k is a common divisor of a and b.

Then $\exists\, a', b'$ $\quad a = a'k$, $b = b'k$. Bézout $\Rightarrow$

$\exists\, s, t$ $\quad \gcd(a,b) = sa + tb = sa'k + tb'k = (sa' + tb')k$ ☺

3. Suppose $\exists$ natural m, n with $3^{1/5} = \frac{m}{n}$, i.e. $3n^5 = m^5$ $(*)$

Expand m and n as products of primes and let

j, k be the multiplicities of 3 in m, n.

From $(*)$ we get $1 + 5k = 5j$, but $5 \nmid 1$ ☹

4. Basis: $n = 1$ $\quad \phi(x) = \phi(x)$ ☺

Inductive step: Let $n > 1$ and assume $\phi(x^{n-1}) = \phi(x)^{n-1}$.

Then $\phi(x^n) = \phi(x^{n-1}x) = \phi(x^{n-1})\,\phi(x) = \phi(x)^{n-1}\phi(x) = \phi(x)^n$ ☺

5. $e = \varphi(e) = \phi(xx^{-1}) = \phi(x)\,\phi(x^{-1})$ $\quad \therefore \phi(x)^{-1} = \phi(x^{-1})$

$n = 0$: $\phi(x^0) = \phi(e) = e = \phi(x)^0$ ☺

$n = -k$, $k > 0$: By above problem $\phi(x^k) = \phi(x)^k$, so

$\phi(x^n) = \phi(x^{-k}) = \phi((x^k)^{-1}) = \phi(x^k)^{-1} = (\phi(x)^k)^{-1} = \phi(x)^{-k} = \phi(x)^n$ ☺

6. $\phi : R \to R \qquad \phi(x) = ax$

Hom: $\phi(x+y) = a(x+y) = ax + ay = \phi(x) + \phi(y)$

Suppose ϕ is 1-1.

If $a = 0$, then $\forall x \quad \phi(x) = 0 \quad (\ker\phi = R)$ $\ddot{\frown}$

If a is a zero div. $\exists x \neq 0, \ ax = 0,$

so $x \in \ker\phi$, so $\ker\phi$ is nontrivial $\ddot{\frown}$

Now suppose ϕ is not 1-1, then $\ker\phi$

is nontrivial, so $\exists x \neq 0, \ \phi(x) = 0,$

i.e. $ax = 0$. $\therefore$ a is zero or zero div. $\ddot{\smile}$

7. Since ϕ is a self-map on a finite set,

ϕ is injective $\Leftrightarrow$ ϕ is surjective.

If ϕ is surjective, $\exists x \quad \phi(x) = 1$, i.e. $ax = 1$, so

a is a unit.

Conversely, suppose a is a unit. Let $y \in R$.

Then $\phi(a^{-1}y) = aa^{-1}y = y$. $\therefore \phi$ is surjective.

$\therefore$ Every nonzero element of R is either a unit

or a zero divisor.

8. $\gcd(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \bmod m$ (Gen. Fermat (Euler))

$ed \equiv 1 \bmod \phi(m) \Rightarrow ed = 1 + k\phi(m)$ for some k

$(a^e)^d = a^{ed} = a^{1+k\phi(m)} = a \cdot (a^{\phi(m)})^k \equiv a \cdot 1^k \equiv a \bmod m$ $\ddot{\smile}$

9. $\langle 11 \rangle = \{11, 21, 31, 41, 1\}$ order 1

Lagrange $\Rightarrow$ index $= \frac{|U(50)|}{5} = \frac{\varphi(2 \cdot 5^2)}{5} = \frac{25-5}{5} = 4$

$3\langle 11 \rangle = \{33, 13, 43, 23, 3\}$ order 4

$7\langle 11 \rangle = \{27, 47, 17, 37, 7\}$ order 4

$9\langle 11 \rangle = \{49, 39, 29, 19, 9\}$ order 2

10. $5x \equiv 2 \bmod 13 \Rightarrow 5x \equiv 15 \bmod 13 \Rightarrow x \equiv 3 \bmod 13$

$2x \equiv 4 \bmod 46 \Rightarrow$ $x \equiv 2 \bmod 23$

$x \equiv 3 \bmod 5$

$m = 13 \cdot 23 \cdot 5 = 1495$

m_i	$M_i = \frac{m}{m_i}$	$M_i \bmod m_i$	$M_i^{-1} \bmod m_i$	a_i	$M_i M_i^{-1} a_i$	mod m
13	115	11	6	3	2070	575
23	65	19	17	2	2210	715
5	299	4	4	3	3588	598

\+

1888 $\rightarrow$ 393

$$\boxed{x \equiv 393 \bmod 1495}$$

File Edit Cell Maxima Equations Algebra Calculus Simplify Plot Numeric Help

```
(%i1) load("dg")$

(%i2) ext_euclid(342,181);
(%o2) [9,-17,1]

(%i3) m:50;
      totient(m);
      create_list(create_list(mod(k*11^i,m),i,1,5),k,[1,3,7,9]);
      create_list(create_list(mod(%[k]^i,m),i,1,4),k,2,4);
(%o3) 50
(%o4) 20
(%o5) [[11,21,31,41,1],[33,13,43,23,3],[27,47,17,37,7],[49,39,29,19,9]]
(%o6) [[[33,13,43,23,3],[39,19,49,29,9],[37,47,7,17,27],[21,11,1,41,31]
],[[27,47,17,37,7],[29,9,39,19,49],[33,23,13,3,43],[41,31,21,11,1]],[[
49,39,29,19,9],[1,21,41,11,31],[49,19,39,9,29],[1,41,31,21,11]]]

(%i7) mods:[13,46/2,5];
      rems:[mod(inv_mod(5,mods[1])*2,mods[1]),4/2,3];
      m:prod(mods[i],i,1,3);
      M:create_list(m/mods[i],i,1,3);
      create_list(mod(M[i],mods[i]),i,1,3);
      create_list(inv_mod(M[i],mods[i]),i,1,3);
      create_list(M[i]*%[i]*rems[i],i,1,3);
      create_list(mod(%[i],m),i,1,3);
      sum(%[i],i,1,3);
      x:mod(%,m);
(%o7) [13,23,5]
(%o8) [3,2,3]
(%o9) 1495
(%o10) [115,65,299]
(%o11) [11,19,4]
(%o12) [6,17,4]
(%o13) [2070,2210,3588]
(%o14) [575,715,598]
(%o15) 1888
(%o16) 393

(%i17) chinese(rems,mods);
       [mod(5*x,13),mod(2*x,46),mod(x,5)];
(%o17) 393
(%o18) [2,4,3]
```

Welcome to wxMaxima   Ready for user input