

Linear Equations and Congruences in PARI

David Whitehouse
California Institute of Technology

1 Linear Equations

`gcd(x,y)` gives the greatest common divisor of the integers x and y .

`bezout(x,y)` outputs a 3-dimensional row vector `[u,v,d]` such that $d = \gcd(x,y)$ and $ux + vy = d$. For example,

```
? bezout(12,39)
%1 = [-3, 1, 3]
```

2 Congruences

PARI can also work with congruences, use the command `Mod(x,y)` to enter in $x \bmod y$. You can then do modular arithmetic in exactly the same way as you would do normal arithmetic. Here are some examples.

```
? Mod(2,12) + Mod(7,12)
%1 = Mod(9, 12)
? Mod(3,7) - Mod(6,7)
%2 = Mod(4, 7)
? Mod(9,17) * Mod(2,17)
%3 = Mod(1, 17)
? Mod(2,8)^3
%4 = Mod(0, 8)
? Mod(7,30)^(-1)
%5 = Mod(13, 30)
```