Friday, March 13, 2015
10:22 AM

When can $eX \equiv 1 \bmod (p-1)(q-1)$ be solved? How?

More generally, to solve

$$eX \equiv 1 \bmod m$$

Start with an assumption:

ASSUME $1 = GCF(e,m)$ (That is, e, m relatively prime)

Use the Euclidean Algorithm to find integers r, s such that

$$r \cdot e + s \cdot m = 1$$

Then of course $m \mid s \cdot m$, so $r \cdot e \equiv 1 \bmod m$

So we're done! (Just use this value of r.)

In the case of RSA, that's all we need; this r becomes the private exponent d.

We can do this more generally:

Suppose we want to solve the equation

$$eX \equiv b \bmod m$$

ASSUME FIRST THAT $GCF(e,m) \mid b$. That is, if $g = GCF(e,m)$ then $b = gk$ for some integer k.

Again using the Euclidean algorithm, find r, s such that

$$r \cdot e + s \cdot m = g$$

Then (multiply by k) $(rk) \cdot e + \underbrace{(sk) \cdot m}_{\text{divisible by } m} = \underbrace{gk}_{=b}$.

$\therefore e \cdot (rk) \equiv b \bmod m$,

So a solution is rk.

Example Solve $90X \equiv 18 \bmod 12$

Use Euclidean Algorithm to find GCF(90, 12):

$90 = 12 \cdot 7 + 6$

$12 = 6 \cdot 2 + 0$

So $6 = GCF(90, 12)$. Note $6 \mid 18$, in fact $\frac{18}{6} = 3$ = this k (later).

Now, $6 = 90 - 12 \cdot 7 = \underbrace{1}_{r} \cdot 90 + \underbrace{(-7)}_{s} \cdot 12$,

and $18 = 3 \cdot 90 + \underbrace{(-21) \cdot 12}_{\text{divisible by } 12}$ (I just multiplied through by $k = 3$ to get the 18 to show up)

So $90 \cdot 3 \equiv 18 \bmod 12$

So $X = 3$ is a solution.

Finally, a comment about the assumptions. In the $ex \equiv 1$ example we assumed e & m were relatively prime; in the $ex \equiv b \bmod m$ example we assumed $GCF(e, m) \mid b$. What if this isn't true?

Suppose we have any sol'n x of the equation $ex \equiv b \bmod m$. Then $ex - b$ is a multiple of m, say $(ex - b) = tm$.

Rewrite: $b = tm - ex$.

The GCF of m and e must divide both m and e, so divides the right-hand side $(tm - ex)$, so divides b. That tells us that our assumption was necessary, that we can only solve $ex \equiv b \bmod m$ if $GCF(e, m) \mid b$.

Bye for now.