

Re: JSH: Factoring and residues

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg03164.html>

- *From:* jstevh@xxxxxxx
 - *Date:* 15 Jul 2006 15:09:52 -0700
-

Tim Peters wrote:

[Proginoskes]

...
Maybe he pulls T out of his colon.

If some integer in his colon needs factoring, that would be fine ;-)

Stripped of "the proofs", the method works like this, given composite odd T to factor:

Pick some integer S coprime to T.

Why coprime? That's what he said, & not worth disputing.

Pick some integer x_{res} in $[1, T)$ coprime to T.

Compute:

$i = (2 * x_{\text{res}})^{-1} \text{ modulo } T$
 $k = \text{mod}(S * i, T)$

Note that i isn't used again. Note that the requirements that T be odd, and that x_{res} be coprime to T, are used to guarantee that the modular inverse of $2 * x_{\text{res}}$ exists.

Pick some factorization of $S + k^2$ as the product of two integers:

$$S + k^2 = f_1 * f_2$$

It's unclear whether a search over all possible such factorizations is intended, but it doesn't matter (it's easy to find cases where no non-trivial factor of T is found no matter which way you pick -- take $T = p * q$ for virtually any "not small" primes p and q).

If f_1 and f_2 don't have the same parity, go back and try other choices for something.

Re: JSH: Factoring and residues

At this point we want to find integer y such that $y^2 + S + k^2$ is a perfect square. Formally set:

$$z^2 - y^2 = (z+y)(z-y) = S + k^2 = f_1 * f_2$$

and solve this system of equations for y and z :

$$z + y = f_1$$

$$z - y = f_2$$

This yields (note that because f_1 and f_2 have the same parity, these yield integers):

$$z = (f_1 + f_2)/2$$

$$y = (f_1 - f_2)/2$$

Compute:

$$x = z - k$$

At this point these things are always true:

x , y , and z are integers

$y^2 + S + k^2$ is a perfect square

$$z = \sqrt{y^2 + S + k^2}$$

$$x^2 - y^2 = S - 2*x*k$$

$$2*S*k = x_res \text{ modulo } T$$

And these things are generally false, although James wishes they were true:

$$x = x_res \text{ modulo } T$$

$$x^2 = y^2 \text{ modulo } T$$

$$1 < \gcd(x+y, T) < T$$

$$1 < \gcd(x-y, T) < T$$

The correct mathematical view is that given S and k , you have an infinite range of possible x_res 's and T 's that will satisfy

$$S = 2x_res*k \text{ mod } T$$

and

$$x^2 - y^2 = 0 \text{ mod } T$$

so you can find an S and k that will work with a particular x_res you choose, your desired residue for x , but there are an infinity of other x_res 's and T 's possible for which S and k will also work.

It's as simple as that and there is no reason for anyone to act like there's a big mathematical mystery here.

That opens the real question of how often when you find S and k for your x_{res} , will you get some other answer coming in, instead as the math shifts to some T other than the one you want, and the good news is that other T 's will tend to be integers of absolute value bigger than yours, which means there are probably strategies for limiting that happening.

Now the mathematics here is simple and I think neat, but the politics are high, so rather than admit that future development is possible, or even bother giving mathematical reasons for how certain things can happen Tim Peters is just pushing the position that it can't work well.

Well, maybe, maybe not, but why one way or the other?

That's why I hate how political this damn field has become as you run into operatives like Peters who are fighting a war—what I call the math wars—and the mathematics is just a pawn in a game about convincing people one way or another.

James Harris

.