

## Re: JSH: Factoring and residues

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg03006.html>

---

- *From:* "Tim Peters" <[tim.one@xxxxxxxxxxxxx](mailto:tim.one@xxxxxxxxxxxxx)>
  - *Date:* Fri, 14 Jul 2006 17:14:06 -0400
- 

[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  $x_{\text{res}}$  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  $x_{\text{res}}$  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.

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

Re: JSH: Factoring and residues

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

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

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

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

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

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

$$x = x_{\text{res}} \text{ modulo } T$$

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

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

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

Because you may never see another one :-), here's an example that works, at  $T=35$ .

Pick:

$$x_{\text{res}} = 1$$

$$S = 1$$

Then  $(2*1)^{-1} = 18 \text{ modulo } 35$ :

$$k = S * \text{that} = 1 * 18 = 18$$

$$S + k^2 = 1 + 18^2 = 325$$

Pick factors of 325 (not all ways work; this way does):

$$f_1 = 25$$

$$f_2 = 13$$

Compute:

$$z = (f_1 + f_2)/2 = 19$$

$$y = (f_1 - f_2)/2 = 6$$

Re: JSH: Factoring and residues

$$x = z - k = 19 - 18 = 1$$

Check:

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

$$\text{Yes: } 19 = \sqrt{6^2 + 1 + 18^2} = \sqrt{361}$$

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

$$\text{Yes: both sides} = -35$$

$$2*S*k = x\_res \text{ modulo } T?$$

$$\text{Yes: } 2*1*18 = 1 \text{ modulo } 35$$

Finally:

$$\gcd(x+y, T) = \gcd(1+6, 35) = 7$$

$$\gcd(x-y, T) = \gcd(1-6, 35) = 5$$

It's also true in this specific case that:

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

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

Those are rarely true, although it's possible that the gcds will find a non-trivial factor even when those fail. For example, if you factor 325 as the product of  $f_1 = -325$  and  $f_2 = -1$ , then:

$$z = -163$$

$$y = -162$$

$$x = -181 \text{ which is congruent to } 29 \text{ modulo } 35, \text{ which isn't } x\_res = 1$$

$$x^2 = 1 \text{ modulo } 35 \text{ but } y^2 = 29 \text{ modulo } 35, \text{ which aren't the same}$$

$$\gcd(x+y, 35) = \gcd(-343, 35) = 7$$

$$\gcd(x-y, 35) = \gcd(-19, 35) = 1$$

So one of the gcds "worked" then anyway. 8 of the 12 (order-sensitive) ways to express 325 as the product of two integers don't work at all — although I believe James would like to ammend his claim to say it also works if  $\gcd(x, T)$  or  $\gcd(y, T)$  reveal a non-trivial factor of  $T$ . That came up on alt.math.undergrad, where I completed James's aborted attempt to factor 35, and showed that the choices he made (before he quit) didn't work. He picked  $f_1=65$  and  $f_2=5$ , and it so happens then that  $y=30$  so that  $\gcd(y, T)=5$ . He latched on to that coincidence as "the reason" for why nothing after that point worked the way he believed it should work.

The fundamental problem here is that his argument for why:

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

must hold is entirely missing, so it's hard to know exactly how he got off track. Most suspicious to my eyes is that from:

$$x^2 = y^2 \text{ modulo } T \text{ [1]}$$

and

$$x^2 - y^2 = S - 2*x*k \text{ [1']}$$

Re: JSH: Factoring and residues

it certainly does follow (and obviously so) that:

$$S - 2*x*k = 0 \text{ modulo } T$$

so

$$S - 2*\text{mod}(x, T)*k = 0 \text{ modulo } T$$

so

$$k = S*(2*\text{mod}(x, T))^{-1} \text{ modulo } T \text{ [2]}$$

And that's reversible: [2]+[1'] implies [1], and the method does satisfy [1'].

But there's no reason to imagine that after formally replacing "mod(x, T)" by the free variable "x\_res" in [2] that:

$$k = S*(2*x\_res)^{-1} \text{ modulo } T \text{ [2']}$$

implies that the x computed by the method satisfies:

$$x = x\_res \text{ modulo } T \text{ [3]}$$

to begin with. If [3] were true, then [3]+[2']+[1'] imply [1]. Alas, [3] is rarely true, and without it the method is just useless poke-and-hope. It could be as shallow as the possibly tempting hope that simply naming the free variable "x\_res" is enough all by itself to ensure that [3] is true :-(

Oh well --- facts don't matter, so back to our scheduled ranting :-)

.