SRQR: Fermat's Theorem, Wilson's Theorem (April 9, 2021)

How does one go about 5.2.2?

Could you go over CC problem #2 from Section 5.2?

Let's work through (a). If $\gcd(a, 35) = 1$, that means that $5 \nmid a$ and $7 \nmid a$. By Fermat's theorem, that means that $a^4 \equiv 1 \pmod 5$ and $a^6 \equiv 1 \pmod 7$. If I raise both sides of the first congruence to the third power, and both sides of the second congruence to the second power, I get:

$$a^{12} \equiv 1 \pmod 5$$
$$a^{12} \equiv 1 \pmod 7$$

which means that $a^{12} - 1$ is divisible by both 5 and 7. Since 5 and 7 are relatively prime, corollary 2 after theorem 2.4 implies that $a^{12} - 1$ is also divisible by $5 \cdot 7 = 35$, ie, $a^{12} \equiv 1 \pmod{35}$.

In example 5.1, we can quickly find pairs a and b to form the congruence relation of $ab \equiv 1 \pmod p$ where p is a prime because 13 is a small prime. When we are dealing with bigger primes, is there a way to quickly identify all the pairs?

Is there a method or algorithm for computing the pairs or do we just try easy pairs and then use our calculator for the more difficult ones?

Is there a simpler way to solve 5.3.3 than by working through each individual pairs modular multiplicative inverse?

I think the best (most systematic and fastest) thing to do is to calculate multiplicative inverses *using the Euclidean algorithm*. It's a little tedious if you're doing it by hand, but it's also good practice with concepts and it's not terrible. If you get a computer to do this for you, you should note that computers can run the Euclidean algorithm very quickly. Also, note that inverses come in pairs (except for 1 and 22, which are both their own inverses). So there are 10 inverse pairs mod 23. That means you "only" need to run the Euclidean algorithm 10 times (as opposed to 22 times, like you might naively imagine). Let's do a few of these calculations:

- To find the inverse of 2 mod 23, I need to find a number x such that $2x \equiv 1 \pmod{23}$. If I run the Euclidean algorithm to find Bézout coefficients for 2 and 23, I'll get the x I want:
$$23 = 2 \cdot 11 + 1$$
$$2 = 1 \cdot 2 + 0$$

which tells me that

$$1 = 23 \cdot 1 + 2 \cdot (-11) \equiv 2 \cdot (-11) \equiv 2 \cdot 12 \pmod{23}.$$

Thus 12 is the inverse of 2.

- To find the inverse of 3 mod 23, we do the same thing now with 3 and 23.

$$\begin{aligned} 23 &= 3 \cdot 7 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

So

$$\begin{aligned} 1 &= 3 \cdot 1 - 2 \cdot 1 \\ &= 3 \cdot 1 - (23 \cdot 1 - 3 \cdot 7) \cdot 1 \\ &= 3 \cdot 8 - 23 \cdot 1 \\ &\equiv 3 \cdot 8 \pmod{23} \end{aligned}$$

so 8 is the inverse of 3.

And so forth. The Euclidean algorithm doesn't take very many steps in any of these cases.

There is another systematic thing you can do which makes use of Fermat's little theorem. The idea is to note that $a^{p-1} \equiv 1 \pmod{p}$ implies that $x = a^{p-2}$ is a solution to the congruence $ax \equiv 1 \pmod{p}$. So we can calculate $a^{p-2} \bmod p$ for each a, using binary exponentiation.

- To calculate the inverse of 2 mod 23, we have to calculate $2^{21} \bmod 23$.

$$\begin{aligned} 2^2 &= 4 \\ 2^4 &= (2^2)^2 = 16 \\ 2^8 &= (2^4)^2 = 256 \equiv 3 \pmod{23} \\ 2^16 &= (2^8)^2 \equiv 3^2 = 9 \pmod{23} \end{aligned}$$

So

$$2^{21} = 2^{16+4+1} = 2^{16}2^4 2^1 = 9 \cdot 16 \cdot 2 \equiv 12 \pmod{12}.$$

Thus 2 and 12 are inverses.

- To calculate the inverse of 3 mod 23, we have to calculate $3^{21} \bmod 23$.

$$\begin{aligned} 3^2 &= 9 \\ 3^4 &= (3^2)^2 = 9^2 = 81 \equiv 12 \pmod{23} \\ 3^8 &= (3^4)^2 \equiv 12^2 = 144 \equiv 6 \pmod{23} \\ 3^16 &= (3^8)^2 \equiv 6^2 \equiv 13 \pmod{23} \end{aligned}$$

So

$$3^{21} = 3^{16+4+1} = 3^{16}3^4 3^1 = 13 \cdot 12 \cdot 3 \equiv 8 \pmod{23}.$$

Thus 3 and 8 are inverses.

And so forth. This feels a little slower to me. It feels like there are more calculations that I can't do in my head as easily (I don't know what 256 mod 23 is off the top of my head, nor do I know what $9 \cdot 16 \cdot 2$ mod 23 is off the top of my head). I prefer using the Euclidean algorithm, but it's up to you!

Yet another, *very ad hoc*, strategy that comes to mind is the following. We're looking for pairs of numbers between 1 and 22 whose product is congruent to 1 mod 23. That means the product has to be 1, 24, 47, 70, 93, 115, ...

- The only way to get 1 is $1 \cdot 1$. Thus 1 is its own inverse.
- The only ways to get 24 are: (a) $2 \cdot 12$, so 2 and 12 are inverses, (b) $3 \cdot 8$, so 3 and 8 are inverses, (c) $4 \cdot 6$, so 4 and 6 are inverses.
- 47 is prime, so we can't get 47.
- The only way to get 70 is $7 \cdot 10$, so 7 and 10 are inverses.

And so forth. But this is not a great strategy. The possible products you have to look at go up through $23 \cdot 21 + 1 = 484$, which is quite a large number and it's not so easy (for me at least) to see its factors. And in general, it's also hard for computers to factor numbers (though probably numbers up to 484 wouldn't take a computer very long).

> In theorem 5.5, I don't understand why they conclude that the prime is of the form $4k + 1$.

Every number is of the form $4k, 4k + 1, 4k + 2$ or $4k + 3$ (by the division algorithm). But numbers of the form $4k = 2(2k)$ or $4k + 2 = 2(2k + 1)$ are both even. Since p is assumed to be odd, it has to be of the form $4k + 1$ or $4k + 3$. The proof rules out $4k + 3$, so we can then conclude that it must be of the form $4k + 1$.

> I am still curious about the significance of the pseudoprimes. Are these numbers particularly "useful" in any way, or are they considered more as an interesting side note to the primes?

The first thing to mention here is that, while Burton makes a precise definition of "pseudoprimes," many others use the word in a more loose sense. In the looser usage, a *probable prime* is a number that shares some property with all prime numbers but not with most composite numbers, and a *pseudoprime* is just a probable prime that happens to composite. Satisfying the conclusion of Fermat's litle theorem is one property that a number might share with all primes but not most composites. But people have found many other properties as well.

If you're mostly interested in pure mathematics, it's tempting to view this idea of probable primes mostly as an interesting side note to the idea of primes. I would caution against this point of view, for two reasons.

The first reason is that, even if you're interested in pure mathematics, note that the core idea here is just looking for properties of prime numbers (such as satisfying Fermat's theorem) which most composite numbers don't have. Finding such properties is something a pure mathematician would be interested in!

The second reason is that probable primes are actually "useful." It's much easier algorithmically to check that something is *probably* a prime than it is to check that it's *actually* a prime, and for some applications, there might be very little practical difference between a number that's actually prime, and a number that's you're 99.9999999% sure is prime. As a result, people working in computational number theory (and, by extension, cryptography and other related fields) do use this idea of probable primes, and many number theory libraries implement probabilistic primality tests.