4 Exponential Congruences and Pseudoprimes

In this section we will develop a couple of important tools that rely on congruences and modular arithmetic, and use them to understand the primes a bit better–and come up with a quick test that will "usually" tell us if a number is prime.

4.1 Fermat's Little Theorem

For further reading on the material in this subsection, consult **Rosen 6.1, PMF 9.1, Stein 2.1.3, 2.4, Shoup 2.7**.

In this section we will prove a few results about congruences modulo a prime number. We already know one such result: if p is a prime, then every number not equivalent to 0 modulo p has a multiplicative inverse modulo p (and this is true *only* if p is prime or 1).

We will start with another result proved by Joseph Lagrange in 1771:

Theorem 4.1 (Wilson's Theorem)**.** *If p is prime, then $(p-1)! \equiv -1 \mod p$.*

Example 4.2. If $p = 5$, then $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \equiv 1 \mod 25$.

If $p = 7$ then $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$. We could multiply this out (it's 720, in fact), but we probably don't want to. It's easier to write

$$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6(4 \cdot 2)(5 \cdot 3) \equiv (-1)(1)(1) \mod 7.$$

That is, we can pair every number with its modular inverse modulo 7, except for $6 \equiv -1$ which is left "stranded." This gives us the idea for the proof.

Proof. When $p = 2$ we can check directly that $1! = 1 \equiv 1 \mod 2$. So let's assume p is an odd prime. Then consider the list of numbers $1, 2, \dots, p-1$. We know that each such integer a has a modular inverse a^{-1}, which must also be on this list.

But we proved that the only numbers which are their own inverses modulo p are 1 and $p - 1 \equiv -1$. (see Lemma 3.30). Thus each integer on the list $2, 3, \dots, p-2$ is the modular inverse of exactly one other integer on the list, and thus we have

$$\prod_{i=2}^{p-2} i = 2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1 \mod p$$

$$(p-1) = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2)(p-1) \equiv 1(p-1) \equiv -1 \mod p.$$

□

Importantly, the converse of this theorem is true–any number with this property is prime.

Theorem 4.3. *If $n \geq 2$ is an integer and $(n-1)! \equiv -1 \mod n$ then n is prime.*

Proof. Suppose n is a composite integer. Then $n = ab$ for some integers a, b with $1 < a, b < n$. From here we can take two approaches:

1. If $a \neq b$ then $ab|(n-1)!$ and thus $(n-1)! \equiv 0 \mod n$, and since $n > 1$ we know that $0 \not\equiv -1 \mod n$. Thus we only need to consider the case where $a = b$.

   If $a = b = 2$ then we can see easily that $(n-1)! = 3! = 6 \equiv 2 \mod 4$ and thus $(n-1)! \not\equiv -1 \mod 4$. So assume $a = b > 2$. Then $ab > 2a$ so $2a$ is a factor in the product $(n-1)!$, and thus $2ab|(n-1)!$ and so does $ab = n$. Thus $(n-1)! \equiv 0 \mod n$.

2. Alternatively, we can suppose that $(n-1)! \equiv -1 \mod n$, implying that $n|(n-1)!+1$ and thus $a|(n-1)!+1$. But $a|(n-1)!$ as well and thus $a|(n-1)!+1-(n-1)! = 1$ and thus $a = 1$, which is a contradiction.

□

Thus we can use Wilson's Theorem to test whether a given number is prime: just compute $(p-1)! \mod p$ and see if the result is $p-1$. Unfortunately, this isn't really a *good* or efficient prime test, since it takes a large amount of computation.

Similar to Wilson's Theorem is Fermat's Little Theorem (which is *not* Fermat's Last Theorem!). The first published proof is due to Leonhard Euler.

Theorem 4.4 (Fermat's Little Theorem)**.** *If p is prime and a is an integer with $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.*

Proof. Consider the $p-1$ integers $a, 2a, \ldots, (p-1)a$. We know that none of these integers are equivalent mod p, since if $ia \equiv ja \mod p$ then since $(p, a) = 1$ we know that $i \equiv j \mod p$. Similarly none of these are divisible by p, since if $p|ja$ then $p|j$.

Thus our list contains one representative of every non-zero equivalence class modulo p. So the product of these $p-1$ integers is equivalent to the product of the first $p-1$ non-zero integers modulo p, and thus we have

$$\prod_{k=1}^{p-1} ka \equiv \prod_{k=1}^{p-1} k \mod p$$

$$a^{p-1} \prod_{k=1}^{p-1} \equiv \prod_{k=1}^{p-1} k = (p-1)! \mod p$$

But since $p \not| (p-1)!$, we know that $((p-1)!, p) = 1$, so we can cancel the $(p-1)!$ from both sides and get

$$a^{p-1} \equiv 1 \mod p.$$

□

Remark 4.5. From the perspective of group theory, this says that the order of any element of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ divides $p-1$ which is the order of this group.

Corollary 4.6. *If p is prime and a is an integer, then $a^p \equiv a \mod p$.*

Proof. If $p \not| a$, then by Fermat's little theorem, $a^{p-1} \equiv 1 \mod p$. Multiplying both sides by a gives $a^p \equiv a \mod p$.

If $p|a$ then $a^p \equiv 0 \equiv a \mod p$. □

Example 4.7. This makes it easy to compute large powers of numbers modulo primes. For instance, suppose we want to compute $2^{700} \mod 7$. We know that $2^6 \equiv 1 \mod 7$ and thus $(2^6)^{(116)} = 2^{696} \equiv 1 \mod 7$, so $2^{700} \equiv 2^4 \equiv 16 \equiv 2 \mod 7$

Corollary 4.8. *If p is a prime and a is an integer with $p \not| a$ then a^{p-2} is an inverse of a modulo p.*

Example 4.9. What is the inverse of 5 modulo 7? It is

$$5^5 \equiv 25 \cdot 25 \cdot 5 \equiv 4 \cdot 4 \cdot 5 \equiv 16 \cdot 5 \equiv 2 \cdot 5 \equiv 3 \mod 7.$$

What is the inverse of 7 modulo 11? It is

$$7^9 \equiv (-4)^9 \equiv -4^9 \equiv - \equiv (4^2)^4 \cdot 4 \equiv -16^4 \cdot 4 \equiv -5^4 \cdot 4 \equiv -25^2 \cdot 4 \equiv -3^2 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \mod 11.$$

Recall that when we were trying to solve linear congruences, we reduced many questions to simply the task of finding modular inverses. Thus we can use Fermat's little theorem to make solving linear congruences easier.

Corollary 4.10. *If a, b are integers and p is prime with $p \not| a$, then the solutions to the congruence $ax \equiv b \mod p$ are the integers $x \equiv a^{p-2}b \mod p$.*

4.2 Pseudoprimes

For further reading on the material in this subsection, consult **Rosen 6.2, Stein 2.4**.

In the last subsection we proved two results about congruences modulo a prime number. Wilson's theorem holds if and only if a number is prime, and thus gives us a (very inefficient) prime test.

Fermat's little theorem also holds for congruences modulo any prime, so we can use it to prove a number is not prime.

Example 4.11. We can show 63 is not prime by calculating

$$2^{62} = 2^{60} \cdot 2^2 = (2^6)^{10} \cdot 2 = 64^{10} \cdot 4 \equiv 1^{10} \cdot 4 \equiv 4 \mod 63.$$

Thus 63 cannot be prime, since $2^{p-1} \equiv 1 \mod p$ for any prime.

Unfortunately, Fermat's little theorem doesn't give a very clear prime test, since the converse is *not* true.

Example 4.12. Let $n = 341 = 11 \cdot 31$. But $2^{340} = 2 \cdot (2^{10})^{34}$ and we know that $2^{10} \equiv 1 \mod 11$ by Fermat's little theorem, so

$$2^{340} \equiv (2^{10})^{34} \equiv 1^3 4 \equiv 1 \mod 341.$$

Thus $2^{341-1} \equiv 1 \mod 341$ even though 341 is not prime.

Remark 4.13. This result is due to Pierre Sarrus in 1919; it was not known that the converse to Fermat's little theorem was false until relatively recently.

Definition 4.14. If b is a positive integer, we say an integer n is *pseudoprime to the base b* if n is composite but $b^n \equiv b \mod n$.

Note that if $(b, n) = 1$ then this is equivalent to $b^{n-1} \equiv 1 \mod n$

Example 4.15. We showed that $341 = 11 \cdot 31$ is pseudoprime to base 2. We can also check that $561 = 3 \cdot 11 \cdot 17$ and $645 = 3 \cdot 5 \cdot 43$ are as well.

Remark 4.16. These are somtimes called "Fermat pseudoprimes" because they pass this particular prime test. There are other tests that can generate false positives; we should discuss Euler pseudoprimes towards the end of the course.

For any given base, there are more primes than there are pseudoprimes by a wide margin; pseudoprimes are fairly rare. However, there are infinitely many pseudoprimes for any base. We prove this for base 2 (Proving it for other bases requires more work but is totally possible).

Lemma 4.17. *If d, n are positive integers with $d|n$, and $b > 1$ is an integer, then $b^d - 1 | b^n - 1$.*

Proof. We know that for any t,

$$x^t - 1 = (x-1)(1 + x + x^2 + \cdots + x^{t-2} + x^{t-1}.$$

Thus

$$b^n - 1 = (b^d - 1)(1 + b^d + b^{2d} + \cdots + b^{n-d}).$$

□

Theorem 4.18. *There are infinitely many pseudoprimes to the base 2.*

Proof. Let $n_1 = 341$ be a pseudoprime to the base 2. Recursively define $n_{k+1} = 2^{n_k} - 1$. We claim that n_k is a pseudoprime to the base 2 for each natural number k.

First we prove by induction that n_k is composite. $n_1 = 11 \cdot 31$ is composite. Assume (for induction) that n_i is composite. Then we can write $n_i = a_i b_i$ with $1 < a_i, b_i < n_i$, and we can write

$$n_{i+1} = 2^{n_i} - 1 = (2^a - 1)(1 + 2^a + \cdots + 2^{n_i - a}).$$

Since $2^a - 1 > 1$ and $1 + 2^a + \cdots + 2^{n_i - a} > 1$, we know that n_{i+1} is composite. Thus, by induction, n_k is composite for each natural number k.

Now we show that $2^{n_k} \equiv 2 \mod n_k$. Again, we use induction. We showed, $2^{n_1} \equiv 2 \mod n_1$. So assume (for induction) that $2^{n_i} \equiv 2 \mod n_i$. This means there is an integer m with $2^{n_i} - 2 = m n_i$.

Then we see that $2^{n_{i+1}-1} = 2^{2^{n_i}-2} = 2^{m n_i}$. Then

$$n_{i+1} = 2^{n_i} - 1 | 2^{m n_i} - 1 = 2^{n_{i+1}-1} - 1.$$

Thus $2^{n_{i+1}-1} \equiv 1 \mod n_{i+1}$, so n_{i+1} is a pseudoprime to the base 2. □

The simplest version of the Fermat test therefore does not work to test whether a number is prime, because it has (admittedly rare) counterexamples.

There is still some hope we can use this Fermat test to test whether a number is prime, by using multiple bases, as follows:

Example 4.19. Let us test the primality of 341 using the base 7. We observe that $7^3 = 343 \equiv 2 \mod 341$, which makes this an eaqy base to work with, especially since we already know facts about 2, like that $2^{10} \equiv 1 \mod 341$. Then we see that

$$7^{340} = (7^3)^{113} \cdot 7 \equiv 2^{113} \cdot 7 \equiv (2^{10})^{11} \cdot 2^3 \cdot 7 \equiv 1^{11} \cdot 8 \cdot 7 \equiv 56 \not\equiv 1 \mod 341.$$

Thus we can see that 341 is not prime because $7^{340} \not\equiv 1 \mod 341$.

This approach usually works, but unfortunately it does not always work.

4.2.1 Carmichael Numbers

Definition 4.20. If n is a positive integer such that $b^{n-1} \equiv 1 \mod n$ for all positive integers b with $(b,n) = 1$, we say n is a *Carmichael number* or an *absolute (Fermat) pseudoprime.*

Example 4.21. We claim that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. Suppose $(b, 561) = 1$. Then $(b,3) = (b,11) = (b,17) = 1$. Thus by Fermat's little theorem, $b^2 \equiv 1 \mod 3, b^{10} \equiv 1 \mod 11$, and $b^{16} \equiv 1 \mod 17$.

Then we see that $b^{560} = (b^2)^{280} \equiv 1 \mod 3$, $b^{560} = (b^{10})^{56} \equiv 1 \mod 11$, and $b^{560} = (b^{16})^{35} \equiv 1 \mod 17$. Thus by the Chinese Remainder Theorem, $b^{560} \equiv 1 \mod 561$.

Carmichael conjectured that there were infinitely many Carmichael numbers in 1912; in 1992, Alford, Granville, and Pomerance proved that if $C(x)$ is the number of Carmichael numbers less than x, then for large x we have $C(x) > x^{2/7}$. We wont' prove this result, but we will prove the easy half of it.

Theorem 4.22. *If $n = \prod_{i=1}^{k} q_i$ for $k > 2$, where the q_i are all distinct primes, and $(q_i - 1)|n-1$ for all i, , then n is a Carmichael number.*

Proof. We can see the proof following from the computation we just did for 561. Suppose b is a positive integer with $(b,n) = 1$. Then $(b, q_i) = 1$ for each i, and thus $b^{q_i - 1} \equiv 1 \mod q_i$ by Fermat's Little Theorem. Since $(q_i - 1)|n-1$, we then have that $b^{n-1} \equiv 1 \mod q_i$ for each i, and the Chinese Remainder Theorem tells us that $b^{n-1} \equiv 1 \mod \prod_{i=1}^{k} q_i$. □

Remark 4.23. The converse of this theorem is also true, but we're not ready to prove it yet.

Thus the proof that there are infinitely many Carmichael numbers reduces to proving that there are infinitely many numbers $n = \prod q_i$ where $q_i - 1 | n - 1$ for each q_i.

Fact: there are 43 Carmichael numbers $\leq 10^6$, and 105,202 that are $\leq 10^{15}$. (That seems like a lot, but 10^{15} is a very large number).

4.2.2 The Miller test

We can push all these arguments a bit farther. We know from your homework that if $x^2 \equiv 1 \mod p$ then $x \equiv \pm 1 \mod p$. So suppose we have some number b such that $b^{n-1} \equiv 1 \mod n$. We can compute $b^{(n-1)/2} \mod n$; if this quantity is not congruent to $\pm 1 \mod n$ then n must not be prime.

Example 4.24. Let $n = 561$ and let $b = 5$. Then we compute that $5^{560} \equiv 1 \mod 561$ as before. But $5^{280} \equiv 67 \not\equiv \pm 1 \mod 561$ so we know that 561 is not prime.

(Note: we can do this by hand but we'd really like a computer).

Definition 4.25. Let n be an integer with $n > 2$ and $n - 1 = 2^s t$ for $s \in \mathbb{N}$ and t odd. We say n passes the *Miller test for the base b* if either $b^t \equiv 1 \mod n$ or if $b^{2^j t} \equiv -1 \mod n$ for some $0 \leq j \leq s - 1$.

Our previous example showed that 561 does not pass the Miller test for the base 5. We now show that $2047 = 23 \cdot 89$ passes the Miller test for the base 2.

Example 4.26. We have $2^{2046} = (2^{11})^{186} = (2048)^{186} \equiv 1 \mod 2047$, so 2047 is pseudoprime to the base 2. Further, we have $2046 = 1023 \cdot 2$, and $2^{1023} = (2^{11})^{93} = (2048)^{93} \equiv 1 \mod 2047$, and thus 2047 passes the Miller test for the base 2.

Theorem 4.27. *If n is prime and b is a positive integer with $n \not| b$, then n passes the Miller test for the base b.*

Proof. Set $n - 1 = 2^s t$ for t odd. Let $x_k = b^{(n-1)/2^k} = b^{2^{s-k}t}$ for $0 \leq k \leq s$, and thus $x_0 = b^{n-1}$. Since n is prime, by Fermat's Little Theorem, we know that $x_0 = b^{n-1} \equiv 1 \mod n$.

We prove the rest by induction (sort of). Fix some $k \leq s$ and suppose (for induction) that $x_1 \equiv 1 \mod n$ for each $i < k$. Then since $(x_k)^2 = (b^{(n-1)/2^k})^2 = b^{(n-1)/2^{k-1}} = x_{k-1} \equiv 1$, we know that $x_k \equiv \pm 1 \mod n$. Thus by induction, either $x_k \equiv 1 \mod n$ for every $k < s$, or $x_k \equiv -1 \mod n$ for some $k \leq s$.

Thus in particular, either $b^{(n-1)/2^k} = b^{t2^k} \equiv -1 \mod n$ for some k, or $b^{(n-1)/2^s} - b^t \equiv 1 \mod n$, so n passes the Miller test for the base b. □

Notice that if n passes the Miller test for the base b, then in particular $b^{n-1} \equiv 1 \mod n$, and thus n is a pseudoprime to the base b. But passing the Miller test is in fact harder, leading us to define:

Definition 4.28. If n is composite and passes the Miller test for the base b, we say n is a *strong pseudoprime to the base b.*

Thus we saw that 2047 is a strong pseudoprime to the base 2.

Theorem 4.29. *There are infinitely many strong pseudoprimes to the base 2.*

Proof. We will claim something more specific: if n is a pseudoprime to the base 2, then $N = 2^n - 1$ is a strong pseudoprime to the base 2. Since there are infinitely many pseudoprimes, there are thus infinitely many strong pseudoprimes.

Suppose n is an odd pseudoprime to the base 2. That is, n is composite and $2^{n-1} \equiv 1 \mod n$. Thus $2^{n-1} - 1 = nk$ for some odd integer k. Then

$$N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2nk$$

is the factorization of N into an odd integer and a power of 2.

But we compute now that $2^n \equiv 1 \mod N$ and thus

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \mod N.$$

Thus $2^{(N-1)/2} \equiv 1 \mod N$, and $(N-1)/2$ is the largest odd factor of $N - 1$, so N passes the Miller test for the base 2.

Now we only need to show that N is composite. But we showed in the proof of Theorem 4.18 that if n is composite then so is $N = 2^n - 1$. Thus N is composite but passes the Miller test for the base 2, and thus is a strong pseudoprime to the base 2. Because there are infinitely many pseudoprimes, there are thus infinitely many strong pseudoprimes. □

Theorem 4.30. *If n is an odd composite positive ingeter, then n passes the Miller test for at most $(n-1)/4$ bases b with $1 \leq b \leq n-1$.*

We need more tools before we can prove this. We can use this result to prove that a number is prime, but it takes far longer than simple trial division. But it produces a good probabilistic primality test:

Theorem 4.31 (Rabin's Probabilistic Primality Test)**.** *Let n be a positive integer. Pick k different postiive integers less than n and perfom the Miller test on n for each of these bases. If n is composite, the probability that n passes all k tests is less than $(1/4)^k$.*

This generates an extremely efficient *probabilistic* test; The odds of a composite number n passing 100 Miller tests are less than 10^{-60}. (Note: always be careful reasoning about p-values: this doesn't mean that a number that passes 100 Miller tests has less than 10^{-60} chance of being composite. The chances are still quite small).

However, if we assume the Generalized Riemann Hypothesis, we can get a good deterministic prime test.

Conjecture 4.32. *For every composite positive integer n, there is a base $b < 2(\log n)^2$ such that n fails the Miller test for the base b.*

If this conjecture is true, the Miller test gives us a very good deterministic primality test, which takes $O((\log n)^5)$ operations.

4.3 Euler's Theorem and composite moduli

For further reading on the material in this subsection, consult **Rosen 6.3, PMF 9.3, Stein 2.1.2, Shoup 2.6-7**.

All the work we've done so far only applies to prime moduli. We'd like to extend or adapt these results to composite moduli. To do this we need to tweak everything slightly.

Definition 4.33. Let n be a positive integer. We define the *Euler phi-function* $\phi(n)$ to be the number of positive integers $\leq n$ that are relatively prime to n.

Example 4.34. $\phi(7) = 6$, since 7 is relatively prime to $1, 2, 3, 4, 5, 6$. $\phi(8) = 4$ since 8 is relatively prime to $1, 3, 5, 7$. $\phi(9) = 6$ since $1, 2, 4, 5, 7, 8$ are relatively prime to 9. $\phi(10) = 4$ since $1, 3, 7, 9$ are relatively prime to 10.

Definition 4.35. A *reduced residue system modulo n* is a set of $\phi(n)$ integers such that each element of the set is relatively prime to n, and no congruence class modulo n is represented more than once.

Example 4.36. $\{1, 2, 3, 4, 5, 6\}$ is a reduced residue system modulo 7. So is $\{2, 4, 6, 8, 10, 12\}$.

$\{1, 3, 5, 7\}$ is a reduced residue system modulo 8. So is $\{-3, -1, 1, 3\}$.

Lemma 4.37. *If $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ is a reduced residue system modulo n and $(a, n) = 1$, then the set $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ is also a reduced residue system modulo n.*

Proof. Suppose $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ is a reduced residue system modulo n, and $(a, n) = 1$.

First we have to prove that $(ar_j, n) = 1$. Suppose $(ar_j, n) > 1$. Then there is some prime p that divides both n and ar_j. But then either $p|a$ or $p|r_j$, so either $p|n$ and $p|a$ and thus $(a, n) \neq 1$; or $p|n$ and $p|r_j$ and thus $(r_j, n) \neq 1$. Either way is a contradiction. Thus $(ar_j, n) = 1$ for each j.

Now we wish to show that if $ar_j \equiv ar_i \mod n$ then $i = j$. But suppose $ar_j \equiv ar_i \mod n$. Then since $(a, n) = 1$, by modular cancellation we know that $r_j \equiv r_i \mod n$, and since $\{r_1, \ldots, r_{\phi(n)}\}$ is a reduced residue system, we know that $r_j \equiv r_i \mod n$ only if $j = i$. □

Theorem 4.38 (Euler's Theorem)**.** *If a, n are natural numbers and $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$.*

Proof. Let $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ be the reduced residue system made up of integers less than n that are relatively prime to n. Then since $(a, n) = 1$, we know the set $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$

is a reduced residue system. Thus the set of least positive residues

$$\{ar_1 \mod n, ar_2 \mod n, \dots, ar_{\phi(n)} \mod n\}$$

must be the set $\{r_1, r_2, \dots, r_{\phi(n)}\}$ in some order (because each set has exactly one representative of each equivalence class).

If we multiply them all together, this tells us that

$$r_1 r_2 \dots r_{\phi(n)} \equiv (ar_1)(ar_2)\dots(ar_{\phi(n)}) \equiv a^{\phi(n)}(r_1 r_2 \dots r_{\phi(n)}) \mod n.$$

But since $(r_i, n) = 1$, we know that $(r_1 r_2 \dots r_{\phi(n)}, n) = 1$, and thus by modular cancellation we have $a^{\phi(n)} \equiv 1 \mod n$ as desired. □

Corollary 4.39. *If a, m are natural numbers with $(a, m) = 1$, then $a^{\phi(m)-1}$ is a multiplicative inverse for a modulo m.*

Example 4.40. Compute $5^{200} \mod 9$.

We know that $5^6 = 5^{\phi(9)} \equiv 1 \mod 9$. Thus

$$5^{100} = 5^{198} \cdot 5^2 = (5^6)^{33} \cdot 25 \equiv 1 \cdot 25 \equiv 7 \mod 9.$$

These results look *suspiciously similar* to Fermat's little theorem and its corollary. In fact Fermat's little theorem is a special case if $\phi(p) = p - 1$, which is in fact the case.

Exercise 4.41. *$\phi(n) = n - 1$ if and only if n is prime.*

Remark 4.42. There are a lot more results we can prove about computing $\phi(n)$, and basically the next big chunk of material will be devoted to that.