Example 128.

(a) Show that 7 is a primitive root modulo 26.

(b) Using the first part, make a complete list of all primitive roots modulo 26.

Solution.

(a) We need to show that 7 has order $\phi(26)=12$.
The order of 7 (or any invertible residue) must divide $\phi(26)=12$. Hence, the only possibilities for orders are $1,2,3,4,6,12$. The fact that $7^4\equiv(-3)^2\equiv 9\not\equiv 1 \pmod{26}$ and $7^6\equiv(-3)^3\equiv -1\not\equiv 1 \pmod{26}$ is enough (why?!) to conclude that the order of 7 must be 12.

(b) Since 7 is a primitive root, all other invertible residues are of the form 7^a.
Recall that 7^a has order $\frac{12}{\gcd(12,a)}$. Thus, 7^a is a primitive root if and only if $\gcd(12,a)=1$.
Therefore, a list of all primitive roots modulo 26 is: $7, 7^5, 7^7, 7^{11}$
[These are $\phi(\phi(26))=\phi(12)=4$ many primitive roots.]

The same logic applies whenever there is at least one primitive root:

Theorem 129. (number of primitive roots) Suppose there is a primitive root modulo n. Then there are $\phi(\phi(n))$ primitive roots modulo n.

Proof. Let x be a primitive root. It has order $\phi(n)$. All other invertible residues are of the form x^a.
Recall that x^a has order $\frac{\phi(n)}{\gcd(\phi(n),a)}$. This is $\phi(n)$ if and only if $\gcd(\phi(n),a)=1$. There are $\phi(\phi(n))$ values a among $1,2,\ldots,\phi(n)$, which are coprime to $\phi(n)$.
In conclusion, there are $\phi(\phi(n))$ primitive roots modulo n. □

Comment. Recall that, for instance, there is no primitive root modulo 8. That's why we needed the assumption that there should be a primitive root modulo n (which is the case if and only if n is of the form $1,2,4,p^k,2p^k$ for some odd prime p).

Corollary 130. There are $\phi(\phi(p))=\phi(p-1)$ primitive roots modulo a prime p.

Example 131. Let p be an odd prime. Show that at most half of the invertible residues modulo p are primitive roots.

Solution. In other words, we need to show that $\frac{\phi(p-1)}{p-1}\leqslant\frac{1}{2}$. Let $p_1,p_2,\ldots$ be the primes, in increasing order, dividing $p-1$. Since $p\neq 2$, $p-1$ is divisible by 2, so that $p_1=2$.
Then, $\phi(p-1)=(p-1)\underbrace{\left(1-\frac{1}{p_1}\right)}_{=1/2}\underbrace{\left(1-\frac{1}{p_2}\right)}_{\leqslant 1}\cdots\leqslant\frac{1}{2}(p-1)$.
Consequently, $\frac{\phi(p-1)}{p-1}\leqslant\frac{\frac{1}{2}(p-1)}{p-1}=\frac{1}{2}$, as claimed.

In fact. Note that $\left(1-\frac{1}{p_2}\right)<1$ if there is a second prime. Our proof therefore actually shows that $\frac{\phi(p-1)}{p-1}=\frac{1}{2}$ if and only if $p-1$ is of the form 2^n (i.e. the only prime dividing $p-1$ is 2). Equivalently, if p is of the form 2^n+1.

Comment. Primes of the form 2^n+1 are known as **Fermat primes**. It can be shown that such a prime is, in fact, necessarily of the form $F_k=2^{2^k}+1$. The first five numbers $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ are prime, and Fermat conjectured that F_k is prime for all $k\geqslant 0$. This was proven wrong by Euler who demonstrated that $F_5=2^{32}+1=641\cdot 6700417$ (this was way before the time, we could ask a computer to factor not-too-large numbers). To this day, it is not known whether any further Fermat primes exist.

Example 132. Recall that, for every prime p, primitive roots exist. The total number of primitive roots is $\phi(\phi(p)) = \phi(p-1)$. The following computations in Sage indicate that typically a "decent" proportion (25-50%) of all invertible residues are primitive roots. The exact proportion is, of course $\frac{\phi(p-1)}{p-1}$ but to say more about the magnitude, we need the factorization of $p-1$.

Advanced comment. However, the number of primitive roots can (though this is very rare) be an arbitrarily small proportion. In fact, a result of Kátai shows that, for each $x \in [0,1]$, there is a proportion $P(x)$ of primes with $\frac{\phi(p-1)}{p-1} \leqslant x$, and that $P(x)$ is a strictly increasing continuous function with $P(0) = 0$ and $P(1/2) = 1$.

```
Sage] prime_range(30)
```

$[2, 3, 5, 7, 11, 13, 17, 19, 23, 29]$

```
Sage] euler_phi(26)
```

12

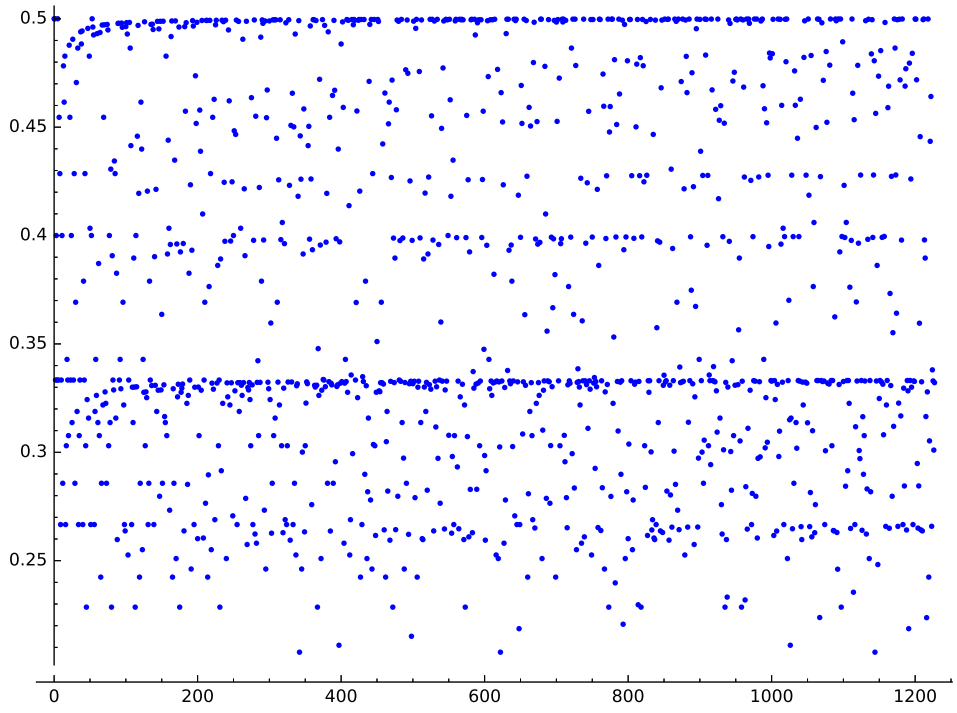
```
Sage] [p^2 for p in prime_range(30)]
```

$[4, 9, 25, 49, 121, 169, 289, 361, 529, 841]$

```
Sage] [euler_phi(p-1)/(p-1) for p in prime_range(30)]
```

$$\left[1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{1}{3}, \frac{1}{2}, \frac{1}{3}, \frac{5}{11}, \frac{3}{7}\right]$$

```
Sage] list_plot([euler_phi(p-1)/(p-1) for p in prime_range(3,10000)])
```



14 Applying the CRT to computing powers

If we know the factorization of the modulus, the CRT speeds up the computation of powers:

Example 133. Compute $3^{29} \pmod{77}$ using the Chinese remainder theorem.

Solution. We determine $x = 3^{29}$ both modulo 7 and 11:

- $3^{29} \equiv 3^5 \equiv 3 \cdot 4 \equiv -2 \pmod 7$ [Here, we used $29 \equiv 5 \pmod{\phi(7)}$ and $3^2 \equiv 2$, $3^4 \equiv 4 \pmod 7$.]
- $3^{29} \equiv 3^{-1} \equiv 4 \pmod{11}$ [Here, we proceeded unusually and used $29 \equiv -1 \pmod{\phi(11)}$.]

Therefore, $x \equiv -2 \pmod 7$ and $x \equiv 4 \pmod{11}$.
Using the Chinese remainder theorem, $x = -2 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 7}}_{2} + 4 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 11}}_{-3} \equiv -128 \equiv 26 \pmod{77}$.

Comment. Alternatively, we can proceed modulo $n = 77$ directly and use binary exponentiation. However, if we already know the factorization of n (that's a big "if" for large n), then applying the Chinese remainder theorem (followed by binary exponentiation) is a little faster.

Example 134. (review) Compute $7^{100} \pmod{60}$.

Solution. $\phi(60) = \phi(2^2)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$. Since $\gcd(7, 60) = 1$, we obtain that $7^{16} \equiv 1 \pmod{60}$ by Euler's theorem. Since $100 \equiv 4 \pmod{16}$, we have $7^{100} \equiv 7^4 \pmod{60}$.
It remains to notice that $7^2 = 49 \equiv -11$ and hence $7^4 \equiv (-11)^2 = 121 \equiv 1 \pmod{60}$. So, $7^{100} \equiv 1 \pmod{60}$.
Comment. The next example shows that we actually have $a^4 \equiv 1 \pmod{60}$ for all integers a coprime to 60.

Euler's theorem doesn't necessarily provide an optimal exponent. For instance:

Example 135. Show that $a^4 \equiv 1 \pmod{60}$ for all integers a coprime to 60.

Note. Since $\phi(60) = \phi(2^2)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$, Euler's theorem shows that $a^{16} \equiv 1 \pmod{60}$.

Proof. By the Chinese remainder theorem, $a^4 \equiv 1 \pmod{60}$ is equivalent to

$$a^4 \equiv 1 \pmod 4, \quad a^4 \equiv 1 \pmod 3, \quad a^4 \equiv 1 \pmod 5.$$

All three of these congruences are true:

- $a^4 \equiv 1 \pmod 5$ is true by Fermat's little theorem.
- $a^4 \equiv 1 \pmod 3$ is true, because $a^2 \equiv 1 \pmod 3$ by Fermat's little theorem.
- $a^4 \equiv 1 \pmod 4$ is true, because $a^2 \equiv 1 \pmod 4$ by Euler's theorem ($\phi(4) = 2$).

(Note that a is coprime to 60 if and only if a is coprime to each of 4, 3, 5.) □

A brute-force verification in Sage. The following computation also proves the claim. Even if you have never coded yourself, you can surely figure out what the following code is doing:

```
Sage] [1..59]
```

$[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59]$

```
Sage] [ x for x in [1..59] if gcd(x,60)==1 ]
```

$[1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59]$

```
Sage] [ power_mod(x,4,60) for x in [1..59] if gcd(x,60)==1 ]
```

$[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]$

Proceeding as in Example 135, we obtain the following result:

Theorem 136. (strengthening of Euler's theorem) Suppose n has the prime factorization $n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$. If $\gcd(a,n) = 1$, then

$$a^{\lambda(n)} \equiv 1 \pmod{n} \qquad \text{where} \quad \lambda(n) = \operatorname{lcm}(\phi(p_1^{r_1}), \phi(p_2^{r_2}), \ldots, \phi(p_m^{r_m})).$$

Advanced. The exponent $\lambda(n)$ in this result is best possible unless n is divisible by 8; see, for instance:
https://en.wikipedia.org/wiki/Carmichael_function
The only improvement that can be made is that, in the computation of $\lambda(n)$, $\phi(2^r)$ may be replaced with $\frac{1}{2}\phi(2^r)$ if $r \geqslant 3$. This is known as Carmichael's theorem.

Example 137. Since $60 = 2^2 \cdot 3 \cdot 5$, we have $\lambda(60) = \operatorname{lcm}(\phi(2^2), \phi(3), \phi(5)) = \operatorname{lcm}(2,2,4) = 4$. By the theorem, $a^4 \equiv 1 \pmod{60}$ whenever $\gcd(a,60) = 1$, as we had observed in Example 135.

Example 138. Based on Euler's theorem and the Chinese remainder theorem, find the smallest exponent k such that $a^k \equiv 1 \pmod{42}$ for all integers a coprime to 42.

Solution. Since $42 = 2 \cdot 3 \cdot 7$, the smallest such exponent is $\lambda(42) = \operatorname{lcm}(\phi(2), \phi(3), \phi(7)) = \operatorname{lcm}(1,2,6) = 6$.

Note. Since $\phi(42) = \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = 12$, this improves the exponent in Euler's theorem by a factor of 2.

Note. In this case, we can easily see that the exponent 6 cannot be further decreased. For instance, take a residue that is a primitive root modulo 7; its order modulo 42 must be at least 6 as well.

Example 139. Based on Euler's theorem and the Chinese remainder theorem, find the smallest exponent $k \geqslant 1$ such that $a^k \equiv 1 \pmod{675}$ for all integers a coprime to 675.

Solution. Since $675 = 3^3 \cdot 5^2$, the smallest such exponent is $\lambda(675) = \operatorname{lcm}(\phi(3^3), \phi(5^2)) = \operatorname{lcm}(18,20) = 180$.

Note. Since $\phi(675) = \phi(3^3)\phi(5^2) = 18 \cdot 20 = 360$, this improves the exponent in Euler's theorem by a factor of 2.

The following is a variation of the same idea we used in Example 135.

Lemma 140. Suppose that m and n are coprime. If $x \pmod{n}$ has multiplicative order r and $x \pmod{m}$ has multiplicative order s, then $x \pmod{mn}$ has multiplicative order $\operatorname{lcm}(r,s)$.

Proof. Suppose that $x^k \equiv 1 \pmod{mn}$. Equivalently, by the CRT, $x^k \equiv 1 \pmod{m}$ as well as $x^k \equiv 1 \pmod{n}$. By Lemma 126, this is further equivalent to $r \mid k$ and $s \mid k$. Clearly, the smallest such k is $k = \operatorname{lcm}(r,s)$. □

Example 141. Determine the order of $2 \pmod{77}$ using the Chinese remainder theorem.

Solution. We first determine the orders of $2 \pmod{7}$ and $2 \pmod{11}$.

- modulo 7 (since $\phi(7) = 6$, the possible orders are $2, 3, 6$): $2^2 \equiv 4$, $2^3 \equiv 4 \cdot 2 \equiv 1$.
  Thus, $2 \pmod{7}$ has order 3.
- modulo 11 (since $\phi(11) = 10$, the possible orders are $2, 5, 10$): $2^2 \equiv 4$, $2^5 \equiv 2^4 \cdot 2 \equiv 5 \cdot 2 \equiv -1 \not\equiv 1$.
  Thus, $2 \pmod{11}$ has order 10.

Taken together, it follows from the lemma that $2 \pmod{77}$ has order $\operatorname{lcm}(3,10) = 30$.

Note. Can you see, from these considerations, why there cannot exist a primitive root modulo 77?

Example 142. Fermat's little theorem can be stated in the slightly stronger form:

$$n \text{ is a prime} \iff a^{n-1} \equiv 1 \pmod{n} \text{ for all } a \in \{1, 2, \ldots, n-1\}$$

Why? Fermat's little theorem covers the "$\Longrightarrow$" part. The "$\Longleftarrow$" part is a direct consequence of the fact that, if n is composite with divisor d, then $d^{n-1} \not\equiv 1 \pmod{n}$. (Why?!)

Review. In the second part, we used that the **contrapositive** of $A \Longrightarrow B$ is the logically equivalent statement $\neg B \Longrightarrow \neg A$.

15 Primality testing

Recall that it is extremely difficult to factor large integers (this is the starting point for many cryptosystems). Surprisingly, it is much simpler to tell if a number is prime.

Example 143. The following is the number mentioned earlier, for which RSA Laboratories, until 2007, offered $100,000 to the first one to factorize it. To this day, nobody has been able to do so.

Has the thought crossed your mind that the challengers might be tricking everybody by choosing M to be a huge prime that cannot be factored further? Well, we'll talk more about primality testing soon. But we can actually quickly convince ourselves that M cannot be a prime. If M was prime then, by Fermat's little theorem, $2^{M-1} \equiv 1 \pmod{M}$. Below, we compute $2^{M-1} \pmod{M}$ and find that $2^{M-1} \not\equiv 1 \pmod{M}$. This proves that M is not a prime. It doesn't bring us any closer to factoring it though.

Comment. Ponder this for a while. We can tell that a number is composite without finding its factors. Both sides to this story (first, being able to efficiently tell whether a number is prime, and second, not being able to factor large numbers) are of vital importance to modern cryptography.

```
Sage] rsa = Integer("135066410865995223349603216278805969938881475605667027524485143851\
                    525610604859533833940287150571909441798207282164471551373680419703\
                    964191743046496589274256239341020864383202110372958725762358509643\
                    110564073501508187510676594629205563685529475213500852879416377328\
                    533906109750544334999811150056977236890927563")

Sage] power_mod(2, rsa-1, rsa)

    1209390944320336158676505953529569968675400984635889512389028083675567339322020593385 3\
    348534147116662841968124107288512373904071077139405352848835710498409193003137847878955\
    226029615123284879513798127406300472693925500331497519103479951096634123177725212482975\
    950196643140069546889855131459759160570963857373851
```

Comment. Just for giggles, let us emphasize once more the need to compute $2^{N-1} \pmod{N}$ without actually computing 2^{N-1}. Take, for instance, the 1024 bit RSA challenge number $N = 135\ldots563$ in this example. The number 2^{N-1} itself has $N - 1 \approx 2^{1024} \approx 10^{308.3}$ binary digits. It is often quoted that the number of particles in the visible universe is estimated to be between 10^{80} and 10^{100}. Whatever these estimates are worth, our number has WAY more digits (!) than that. Good luck writing it out! [Of course, the binary digits are a single 1 followed by all zeros. However, we need to further compute with that!]

Comment. There is nothing special about 2 in this discussion. You could just as well use, say, 3.

Fermat primality test

Input: number n and parameter k indicating the number of tests to run

Output: "not prime" or "likely prime"

Algorithm:

Repeat k times:
  Pick a random number a from $\{2, 3, \ldots, n-2\}$.
  If $a^{n-1} \not\equiv 1 \pmod{n}$, then stop and output "not prime".
Output "likely prime".

If $a^{n-1} \equiv 1 \pmod{n}$ although n is composite, then a is called a **Fermat liar** modulo n.

On the other hand, if $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite and a is called a **Fermat witness** modulo n.

Flaw. There exist certain composite numbers n (see Definition 145) for which every a is a Fermat liar (or reveals a factor of n). For this reason, the Fermat primality test should not be used as a general test for primality. That being said, for very large random numbers, it is exceedingly unlikely to meet one of these troublesome numbers, and so the Fermat test is indeed used for the purpose of randomly generating huge primes (for instance in PGP). In fact, in that case, we can even always choose $a = 2$ and $k = 1$ with virtual certainty of not messing up.

There do exist extensions of the Fermat primality test which solve these issues.

[For instance, Miller-Rabin, which checks whether $a^{n-1} \equiv 1 \pmod{n}$ but also checks whether values like $a^{(n-1)/2}$ are congruent to ± 1.]

Advanced comment. If n is composite but not an absolute pseudoprime (see Definition 145), then at least half of the values for a satisfy $a^{n-1} \not\equiv 1 \pmod{n}$ and so reveal that n is not a prime. This is more of a theoretical result: for most large composite n, almost every a (not just half) will be a Fermat witness.

Example 144. Suppose we want to determine whether $n = 221$ is a prime. Simulate the Fermat primality test for the choices $a = 38$ and $a = 24$.

Solution.

- First, maybe we pick $a = 38$ randomly from $\{2, 3, ..., 219\}$.
  We then calculate that $38^{220} \equiv 1 \pmod{221}$. So far, 221 is behaving like a prime.
- Next, we might pick $a = 24$ randomly from $\{2, 3, ..., 219\}$.
  We then calculate that $24^{220} \equiv 81 \not\equiv 1 \pmod{221}$. We stop and conclude that 221 is not a prime.

Important comment. We have done so without finding a factor of n. (To wit, $221 = 13 \cdot 17$.)

Comment. Since 38 was giving us a false impression regarding the primality of n, it is called a **Fermat liar** modulo 221. Similarly, we say that 221 is a **pseudoprime** to the base 38.

On the other hand, we say that 24 was a **Fermat witness** modulo 221.

Comment. In this example, we were actually unlucky that our first "random" pick was a Fermat liar: only 14 of the 218 numbers (about 6.4%) are liars. As indicated above, for most large composite numbers, the proportion of liars will be exceedingly small.

Somewhat suprisingly, there exist composite numbers n with the following disturbing property: every residue a is a Fermat liar or $\gcd(a, n) > 1$.

This means that the Fermat primality test is unable to distinguish n from a prime, unless the randomly picked number a happens to reveal a factor (namely, $\gcd(a, n)$) of n (which is exceedingly unlikely for large numbers).

[Recall that, for large numbers, we do not know how to find factors even if that was our primary goal.]

Such numbers are called absolute pseudoprimes:

Definition 145. A composite positive integer n is an **absolute pseudoprime** (or Carmichael number) if $a^{n-1} \equiv 1 \pmod{n}$ holds for each integer a with $\gcd(a, n) = 1$.

The first few are $561, 1105, 1729, 2465, ...$ (it was only shown in 1994 that there are infinitely many of them).

These are very rare, however: there are 43 absolute pseudoprimes less than 10^6. (Versus $78,498$ primes.)

Example 146. Show that 561 is an absolute pseudoprime.

Solution. (using the strengthening of Euler's theorem) We need to show that $a^{560} \equiv 1 \pmod{561}$ for all invertible residues a modulo 561. Since $561 = 3 \cdot 11 \cdot 17$ and $\operatorname{lcm}(\phi(3), \phi(11), \phi(17)) = \operatorname{lcm}(2, 10, 16) = 80$, it follows from Theorem 136 that $a^{80} \equiv 1 \pmod{561}$ for all invertible residues a modulo 561. Since 560 is a multiple of 80, it follows that $a^{560} \equiv 1 \pmod{561}$.

Solution. (direct) We need to show that $a^{560} \equiv 1 \pmod{561}$ for all invertible residues a modulo 561.

Since $561 = 3 \cdot 11 \cdot 17$, $a^{560} \equiv 1 \pmod{561}$ is eqivalent to $a^{560} \equiv 1 \pmod{p}$ for each of $p = 3, 11, 17$.

By Fermat's little theorem, we have $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$. Since $2, 10, 16$ each divide 560, it follows that indeed $a^{560} \equiv 1 \pmod{p}$ for $p = 3, 11, 17$.

Comment. Korselt's criterion (1899) states that what we just observed in fact characterizes absolute pseudoprimes. Namely, a composite number n is an absolute pseudoprime if and only if n is squarefree, and for all primes p dividing n, we also have $p-1 | n-1$.

Comment. Our argument above shows that, in fact, $a^{80} \equiv 1 \pmod{561}$ for all invertible residues a modulo 561. Note

Theorem 147. (Korselt's Criterion) A composite positive integer n is an absolute pseudoprime if and only if n is squarefree and $(p-1) | (n-1)$ for each prime divisor p of n.

Proof. Here, we will only consider the "if" part (the "only if" part is also not hard to show but the typical proof requires a little more insight into primitive roots than we currently have).

To that end, assume that n is **squarefree** and that $(p-1) | (n-1)$ for each prime divisor p of n. Let a be any integer with $\gcd(a, n) = 1$. We will show that $a^{n-1} \equiv 1 \pmod{n}$.

n being squarefree means that its prime factorization is of the form $n = p_1 \cdot p_2 \cdots p_d$ for distinct primes p_i (this is equivalent to saying that there is no integer $m > 1$ such that $m^2 | n$). By Fermat's little theorem $a^{p_i - 1} \equiv 1 \pmod{p_i}$ and, since $(p_i - 1) | (n-1)$, we have $a^{n-1} \equiv 1 \pmod{p_i}$ for all p_i. It therefore follows from the Chinese remainder theorem that $a^{n-1} \equiv 1 \pmod{n}$. □

Comment. Modulo a prime p, Fermat's little theorem implies that $a^p \equiv a \pmod{p}$ for each integer a. (Why?!) It therefore follows from the above argument that, for an absolute pseudoprime n, we have $a^n \equiv a \pmod{n}$ for each integer a (and this property characterizes absolute pseudoprimes).

Example 148. Using Sage, determine all numbers n up to 5000, for which 2 is a Fermat liar.

```
Sage] def is_fermat_liar(x, n):
          return not is_prime(n) and power_mod(x, n-1, n) == 1

Sage] [ n for n in [1..5000] if is_fermat_liar(2, n) ]
```

$$[341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681]$$

Even if you have never written any code, you can surely figure out what's going on!