To begin with we will need to following facts.

Fact 1:

Let $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ be the decomposition of the number n into primes $p_1, \ldots, p_k$. Then

$$a \equiv b \pmod{n}$$

if and only if

$$\begin{aligned} a &\equiv b \pmod{p_1^{a_1}} \\ &\vdots \\ a &\equiv b \pmod{p_k^{a^k}}. \end{aligned} \tag{1}$$

Proof:

Suppose $a \equiv b \pmod{n}$. Then $p_1^{a_1} \cdot \ldots \cdot p_k^{a_k} \mid (a-b)$. Since $p_i^{a_i} \mid p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ for each $i \in \{1, \ldots, k\}$ we find $p_i^{a_i} \mid (a-b)$ for each $i \in \{1, \ldots, k\}$. Thus the Congurences 1 hold.

Conversely suppose the Congruences 1 hold. Then $p_i^{a_i} \mid (a-b)$ for each $i \in \{1, \ldots, k\}$. Thus $a \equiv b \pmod{n}$.

Fact 2:

In a field if $ab = 0$ then either $a = 0$ or $b = 0$.

Proof:

Suppose $ab = 0$. If $a \neq 0$ then there exists an element a^{-1} in the field such that $a^{-1} \cdot a = 1$. This implies

$$b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0.$$

Therefore either a or b is zero.

Next we turn our attention to the exercises.

Question 1:

Let R be the set of elements of the form $a + b\sqrt{-11}$, where a and b are in $\mathbb{Z}$. An element p of R is said to be a prime in R if any divisor of p in R is either $1, -1, p$, or $-p$. Show that $p = 3$ is a prime in R. Find elements a and b in R such that $p = 3$ divides ab but p divides neither a nor b. (This shows that the analogue of Gauss's lemma fails to be true in R.)

Solution:

First we will show that 3 is prime. Consider the function $f : R \to \mathbb{Z}$ defined by $f(a + b\sqrt{-1}) = a^2 + 11b^2$. This is called the *norm* function. One can check that

$$f((a + b\sqrt{-11})(c + \sqrt{-11}d)) = f(a + b\sqrt{-11})f(c + \sqrt{-11}d).$$

To check this, notice

$$\begin{aligned} f((a + b\sqrt{-11})(c + \sqrt{-11}d)) &= f(ac - 11bd + \sqrt{-11}(ad + bc)) \\ &= (ac - 11bd)^2 + 11(ad + bc)^2 \\ &= a^2c^2 + 11^2b^2d^2 + 11a^2d^2 + 11b^2c^2 \\ &= (a^2 + 11b^2)(c^2 + 11d^2) \\ &= f(a + b\sqrt{-11})f(c + \sqrt{-11}d). \end{aligned}$$

Suppose

$$3 = (a + b\sqrt{-11})(c + d\sqrt{-11}) \tag{2}$$

for some integers a, b, c and d.Then

$$9 = f(3) = f((a + b\sqrt{-11})(c + d\sqrt{-11})) = f(a + b\sqrt{-11})f(c + d\sqrt{-11}).$$

However, as $f(a + b\sqrt{-11})$ and $f(c + d\sqrt{-11})$ are integers we find $f(a + b\sqrt{-11}) = 1, 3$ or 9. Notice that

1. if $f(a+b\sqrt{11}) = 1$ then $a+b\sqrt{-11} = \pm 1$,
2. if $f(a+b\sqrt{11}) = 9$ then $a+b\sqrt{-11} = \pm 3$, and
3. $f(a+b\sqrt{11}) = a^2+11b^2$ can never equal 3.

Thus $a+b\sqrt{11} = \pm 1$ or ± 3. Similarly $c+d\sqrt{11} = \pm 1$ or ± 3. Therefore 3 is prime in R.

Alternate, (less elegant) way to show 3 is prime. Suppose

$$3 = (a+b\sqrt{-11})(c+d\sqrt{-11}) \tag{3}$$

for some integers a, b, c and d.

We wish to show that $(a+b\sqrt{-11}), (c+d\sqrt{-11}) \in \{\pm 1, \pm 3\}$. Indeed, expanding the equation we find:

$$\begin{aligned} 3 &= ac - 11bd \quad \text{and} && (4) \\ 0 &= ad + bc && (5) \end{aligned}$$

Suppose first that $b \neq 0$ then by Equation 5 we find

$$c = \frac{-ad}{b}$$

Substituting this back into Equation 4 gives:

$$\begin{aligned} 3 &= \frac{-a^2d}{b} - 11bd \\ &= \left(\frac{a^2}{b^2} + 11\right)(-bd). \end{aligned}$$

As bd is an integer and $|\frac{a^2}{b^2} + 11| > 11$ this is clearly impossible.

We now suppose that $b = 0$. Then by Equation 4 we find $3 = ac$. Thus $a \neq 0$ and so by Equation 5 we have $d = 0$. The Equation 3 now reduces to $3 = ac$ with a, c integers. Since 3 is a prime in the integers, $a, c \in \{\pm 1, \pm 3\}$.

Now, to solve the second part of the exercise. Notice that $3|(a+b\sqrt{-11})$ if and only if $3|a$ and $3|b$. Consider the product:

$$\begin{aligned} (1+\sqrt{-11})(2+\sqrt{-11}) &= (2-11) + (1+2)\sqrt{-11} \\ &= -9 + 3\sqrt{-11}. \end{aligned}$$

Thus $3|(1+\sqrt{-11})(2+\sqrt{-11})$, but $3 \nmid (2+\sqrt{-11})$ and $3 \nmid (1+\sqrt{-11})$. Thus Gauss' lemma fails in R.

Question 2:

An integer is said to be N-smooth if all its prime divisors are less than or equal to N. Show that

$$\prod_{p \leq N} (1 - \tfrac{1}{p})^{-1} = \sum_{n \geq 1, N \text{ smooth}} \frac{1}{n}$$

where the product on the left is taken over the primes less than N, and the (infinite) sum on the right is taken over all the N-smooth integers $n \geq 1$. (Hint: remember how to sum an infinite geometric series! Note also the crucial role played by the fundamental theorem of arithmetic in your argument.)

Solution:

The statement is empty for $N = 1$. Let $p_1, p_2, \ldots$ denote the prime numbers ordered so that $p_i < p_{i+1}$.

We claim that:

$$\prod_{i=1}^{n} (1 - \tfrac{1}{p_i})^{-1} = \sum_{a_1, \ldots, a_n \in \mathbb{N}} \frac{1}{p_1^{a_1} \cdots p_n^{a_n}}$$

We show this by induction on n.

The case $n = 1$ holds since it is the formula for the sum of a geometric series. Suppose it holds for $n = k$, we wish to show it holds for $n = k + 1$. We have by induction:

$$\prod_{i=1}^{k+1}(1 - \tfrac{1}{p_i})^{-1} = \left(\sum_{a_1,\ldots,a_k \in \mathbb{N}} \frac{1}{p_1^{a_1} \cdots p_k^{a_k}} \right) \left(\sum_{a_{k+1} \in \mathbb{N}} \frac{1}{p_{k+1}^{a_{k+1}}} \right)$$

As these are absolutely convergent series, we may (freely) rearrange terms while taking the product. The previous equation can thus be written as:

$$\prod_{i=1}^{k+1}(1 - \tfrac{1}{p_i})^{-1} = \left(\sum_{a_1,\ldots,a_{k+1} \in \mathbb{N}} \frac{1}{p_1^{a_1} \cdots p_{k+1}^{a_{k+1}}} \right)$$

This completes the induction.

Now, if p_n is the largest prime less than N then:

$$\prod_{p \le N}(1 - \tfrac{1}{p})^{-1} = \prod_{i=1}^{n}(1 - \tfrac{1}{p_i})^{-1} = \sum_{a_1,\ldots,a_n \in \mathbb{N}} \frac{1}{p_1^{a_1} \cdots p_n^{a_n}}$$

Notice by the Fundamental Theorem of Arithmetic that the N-smooth numbers are precisely the numbers

$$p_1^{a_1} \cdots p_n^{a_n}.$$

We see that

$$\prod_{p \le N}(1 - \tfrac{1}{p})^{-1} = \sum_{n \ge 1, N \text{ smooth}} \frac{1}{n}$$

(again as the series is absolutely convergent, the order of the summation can be ignored).

Question 3:

Show that

$$\lim_{N \to \infty} \left(\prod_{p \le N}(1 - \tfrac{1}{p})^{-1} \right) = \infty.$$

and conclude that there are infinitely many primes. This remarkable proof was discovered by Leonhard Euler.

Solution:

Notice that the numbers from $1, \ldots, N$ are always N-smooth numbers. This means that the sum

$$\sum_{n \ge 1, N \text{ smooth}} \frac{1}{n} \ge \sum_{n=1}^{N} \frac{1}{n}.$$

However, we know the harmonic series diverges; that is,

$$\lim_{N \to \infty} \sum_{n=1}^{N} \frac{1}{n} = \infty.$$

Thus by the Comparison Test this proves

$$\lim_{N \to \infty} \sum_{n \ge 1, N \text{ smooth}} \frac{1}{n} = \infty.$$

However, by the previous Exercise this proves

$$\lim_{N \to \infty} \prod_{p \le N}(1 - \tfrac{1}{p})^{-1} = \infty.$$

If there were only finitely many primes then the product on the left hand side would be finite. Therefore, this the product on the left must be a product of infinitely many terms which proves there are infinitely many primes.

Question 4:

Solve the following congruence equations:

1. $3x \equiv 5 \pmod 7$
2. $3x \equiv 1 \pmod{11}$
3. $3x \equiv 6 \pmod{15}$
4. $6x \equiv 14 \pmod{21}$.

Solution:

First we will find a solution to $3x \equiv 5$ modulo 7. We know by Fermat's Little Theorem that $3^6 \equiv 1$ modulo 7. Thus

$$3 \cdot 3^5 \equiv 1 \pmod 7.$$

Multiplying both sides by 5 we find

$$3 \cdot 3^5 \cdot 5 \equiv 5 \pmod 7.$$

Thus $3^5 \cdot 5$ is a solution to $3x \equiv 5$ modulo 7. We can simplify the number $3^5 \cdot 5$ as follows:

$$3^5 \cdot 5 \equiv (3^2 \cdot 3^2 \cdot 3) \cdot 5 \equiv 2 \cdot 2 \cdot 3 \cdot 5 \equiv 60 \equiv 4 \pmod 7.$$

Thus 4 is a solution to $3x \equiv 5$ modulo 7.

Next we will find a solution to $3x \equiv 1$ modulo 11. By Fermat's Little Theorem that $3^{10} \equiv 1$ modulo 11. Thus

$$3 \cdot 3^9 \equiv 1 \pmod 7.$$

Thus 3^9 is a solution to $3x \equiv 1$ modulo 11. We can simplify the number 3^9 as follows:

$$3^9 \equiv 3^2 \cdot 3^2 \cdot 3^2 \cdot 3^2 \cdot 3 \equiv (-2) \cdot (-2) \cdot (-2) \cdot (-2) \cdot 3 \equiv 48 \equiv 4 \pmod{11}.$$

Thus $x \equiv 4$ is a solution to $3x \equiv 1 \pmod{11}$.

Now we will find a solution to $3x \equiv 6$ modulo 15. This is the same as finding the elements between 0 and 14 which are solutions to $x \equiv 2$ modulo 5. Clearly, 2 is a solution. As $2 \equiv 7 \equiv 12$ modulo 5, these are the other solutions to $x \equiv 2$ modulo 5. Thus $x \equiv 2, 7, 12$ are the solutions to $3x \equiv 6$ modulo 15.

The congruence $6x \equiv 14$ modulo 21 has no solution because no matter what number we choose for x the left hand side $6x$ is divisible by 3, while the other side of the congruence 14 is not divisible by 3.

Question 5:

Show that $a^5 \equiv a \pmod{30}$, for all integers a.

Solution:

By Fact 1 it suffices to show the following congruences hold:

$$a^5 \equiv a \pmod 2 \tag{6}$$
$$a^5 \equiv a \pmod 3 \tag{7}$$
$$a^5 \equiv a \pmod 5 \tag{8}$$

First we will show Congruence 6 holds. Clearly it holds if $a \equiv 0 \pmod 2$. If $a \not\equiv 0 \pmod 2$ then $a \equiv 1 \pmod 2$. This means a is an odd number, and so a^5 is also an odd number. Thus $a^5 \equiv 1 \pmod 2$. In either case we find Congruence 6 holds.

Next we will show Congruence 7 holds. Again it holds if $a \equiv 0 \pmod 3$. If $a \not\equiv 0 \pmod 3$ then by Fermat's Little Theorem $a^2 \equiv 1 \pmod 3$. Thus

$$a^5 \equiv a^{2 \cdot 2+1} \equiv (a^2)^2 \cdot a \equiv 1^2 \cdot a \equiv a \pmod 3.$$

Thus in either case we find Congruence 7 holds.

Finally Congruence 8 is exactly Fermat's Little Theorem in the case $p = 5$. Thus as the we have proven the Congruences 6-8 hold. This proves our statement.

Question 6:

Find an element a of $\mathbb{Z}_{11}$ such that every non-zero element of $\mathbb{Z}_{11}$ is a power of a. (An element with this property is called a primitive root mod 11.) Can you do the same in $\mathbb{Z}_{24}$?

Solution:

Notice that

$$\begin{aligned}
2^0 &\equiv 1 && \pmod{11}\\
2^1 &\equiv 2 && \pmod{11}\\
2^2 &\equiv 4 && \pmod{11}\\
2^3 &\equiv 8 && \pmod{11}\\
2^4 &\equiv 16 \equiv 5 && \pmod{11}\\
2^5 &\equiv 2^4 \cdot 2 \equiv 5 \cdot 2 \equiv 10 && \pmod{11}\\
2^6 &\equiv 2^5 \cdot 2 \equiv 10 \cdot 2 \equiv 20 \equiv 9 && \pmod{11}\\
2^7 &\equiv 2^6 \cdot 2 \equiv 9 \cdot 2 \equiv 18 \equiv 7 && \pmod{11}\\
2^8 &\equiv 2^7 \cdot 2 \equiv 7 \cdot 2 \equiv 14 \equiv 3 && \pmod{11}\\
2^9 &\equiv 2^8 \cdot 2 \equiv 3 \cdot 2 \equiv 6 && \pmod{11}\\
2^10 &\equiv 2^9 \cdot 2 \equiv 6 \cdot 2 \equiv 12 \equiv 1 && \pmod{11}
\end{aligned}$$

As every non-zero element of $\mathbb{Z}_{11}$ occurs as a power of 2 we have shown 2 is a primative root mod 11.

Notice that in $\mathbb{Z}_{24}$ there are both invertible elements and non-invertible elements. If a is an invertible element then $\gcd(a, 24) = 1$. Thus $\gcd(a^n, 24) = 1$ for any power n. This proves a cannot generate all the elements because it will never generate the non-invertible elements.

On the other hand, if a is a non-invertible element then $\gcd(a, 24) \neq 1$. Thus $\gcd(a^n, 24) \neq 1$ for any power n. This proves a cannot generate all the elements because it will never generate the invertible elements. Therefore no matter which element we choose it will never be able to generate all the non-zero elements.

Even more than this is true, however. As $a^2 \equiv 1$ for every invertible element, there does not exist an invertible element which could generate all the invertible elements.

Question 7:

Prove or disprove: if $x^2 \equiv 1$ in $\mathbb{Z}_n$, and n is prime, then $x \equiv 1$ or $x \equiv -1 \pmod{n}$. What if n is not prime?

Solution:

Notice that

$$x^2 - 1 \equiv (x+1)(x-1).$$

Since $\mathbb{Z}_n$ is a field when n is a prime, by Fact 2 the above equation proves $x + 1 = 0$ or $x - 1 = 0$. Thus $x \equiv 1$ or $x \equiv -1 \pmod{n}$.

If n is not a prime then $\mathbb{Z}_n$ is not a field. Hence we cannot use Fact 2. In this case the statement is false. A counter-example to the statement in the case where n is composite occurs when $n = 8$. Here $3^2 \equiv 1 \pmod{8}$, although $3 \not\equiv \pm 1 \pmod{8}$.

Question 8:

List the invertible elements of $\mathbb{Z}_5$ and $\mathbb{Z}_{12}$.

Solution:

The invertible elements in $\mathbb{Z}_n$ are those which are relatively prime to n.
In $\mathbb{Z}_5$ the invertible elements are $\overline{1}, \overline{2}, \overline{3}$ and $\overline{4}$, where the bar denotes the equivalence class (mod 5).
In $\mathbb{Z}_{12}$ the invertible elements are $\overline{1}, \overline{5}, \overline{7}$ and $\overline{11}$, where the bar denotes the equivalence class (mod 12).

Question 9:

Show that p is prime if and only if p divides the binomial coefficient $\binom{p}{k}$ for all $1 < k < p$.

Solution:

We will assume that we know that the binomial coefficient is an integer. Suppose p is a prime number. Recall the formula for the binomial coefficient:

$$\binom{p}{k} = \frac{1 \cdot \ldots \cdot p}{(1 \cdot \ldots \cdot k)(1 \cdot \ldots \cdot (p-k))}.$$

As $k < p$ it is clear that $p \nmid (1 \cdot \ldots \cdot k)$. As $k > 1$ it is also clear that $p \nmid (1 \cdot \ldots \cdot (p-k))$. Thus p does not divide the denominator of the equation above. However, p divides the numerator. Therefore p divides the binomial coefficient $\binom{p}{k}$ for any $1 < k < p$.

Conversely suppose p is not a prime number. Then we need to show that there exists at least one natural number k where $1 < k < p$ such that p does not divide the binomial coefficient $\binom{p}{k}$. To do this choose a prime q that divides p and let $m = \frac{p}{q}$, so that $p = mq$. Then choose $k = (m-1)q$. This means

$$\begin{aligned}\binom{p}{k} &= \binom{mq}{(m-1)k} \\ &= \frac{1 \cdot \ldots \cdot (m-1)q \cdot ((m-1)q+1) \cdot \ldots \cdot mq}{(1 \cdot \ldots \cdot (m-1)q)(1 \cdot \ldots \cdot (mq-(m-1)q))}\end{aligned}$$

Cancelling off $(1 \cdot \ldots \cdot (m-1)q)$ from both the numerator and denominator proves

$$\binom{p}{k} = \frac{((m-1)q+1) \cdot \ldots \cdot mq}{1 \cdot \ldots \cdot q}$$

Notice the only number in the set $\{(m-1)q+1, (m-1)q+2, \ldots, mq\}$ which is a multiple of q is the number mq. Thus q divides both the numerator and dominator exactly once, which means $p \nmid \binom{p}{k}$. Thus if p is not prime then p does not divide the binomial coefficient $\binom{p}{k}$ for all $1 < k < p$. This proves the converse to the statement.

Question 10:

Using the result of Exercise 9, prove that if p is prime, then $a^p \equiv a \pmod{p}$ for all integers a (Fermat's little theorem) by induction on a.

Solution:

We will prove this separately for positive and negative numbers.

For the positive case we will use induction. Firstly, this is true in the case where $a = 0$ which is the base case for our induction in both cases. Now for the purpose of induction suppose that $k^p \equiv k \pmod{p}$, we would like to show that $(k+1)^p \equiv k+1 \pmod{p}$.

Indeed we have:

$$(k+1)^p = k^p + \binom{p}{1} k^{p-1} + \cdots + \binom{p}{p-1} k^{p-1} + 1.$$

And by the previous exercise $\binom{p}{\ell} k^{p-1} \equiv 0 \pmod{p}$ for $1 \leq \ell \leq p-1$ and thus

$$k^p + \binom{p}{1} k^{p-1} + \cdots + \binom{p}{p-1} k^{p-1} + 1 \equiv k^p + 1 \pmod{p}.$$

By our inductive assumption we know that $k^p \equiv k$ modulo p, thus

$$(k+1)^p \equiv k+1 \pmod{p}.$$

This proves the inductive step for positive numbers and thus completes the proof for this case.

To prove the result for the negative case notice that since:

$$(-a)^p = (-1)^p a^p \equiv (-1)^p a \pmod{p}$$

it suffices to show that $(-1)^p \equiv -1 \pmod{p}$. In the event that p is odd we have $(-1)^p = -1$ and this completes the result. In that event that p is even, that is $p = 2$, we have $(-1)^2 \equiv 1 \equiv -1 \pmod{2}$ and the result again holds. This proves the result for negative numbers

Question 11:

Show that if $n = 1729$, then $a^n \equiv a \pmod{n}$ for all a, even though n is not prime. Hence the converse to Exercise 10 is not true.

Solution:

First notice 1729 has the prime decomposition

$$1729 = 7 \cdot 13 \cdot 19.$$

Thus by Fact 1 we see that

$$a^{1729} \equiv a \pmod{1729}$$

if and only if

$$a^{1729} \equiv a \pmod{7} \tag{9}$$

$$a^{1729} \equiv a \pmod{13} \tag{10}$$

$$a^{1729} \equiv a \pmod{19} \tag{11}$$

By Fermat's Little Theorem we know that

$$a^6 \equiv 1 \pmod{7}.$$

Thus

$$a^{1729} \equiv a^{6\cdot 288+1} \equiv (a^6)^{288} \cdot a \equiv 1^{288} \cdot a \equiv a \pmod{7}.$$

This proves Congruence 9.

Next we will prove Congruence 10. By Fermat's Little Theorem we know that

$$a^{12} \equiv 1 \pmod{13}.$$

Thus

$$a^{1729} \equiv a^{12\cdot 144+1} \equiv (a^{12})^{144} \cdot a \equiv 1^{144} \cdot a \equiv a \pmod{13}.$$

This proves Congruence 10.

Finally we will prove Congruence 11. By Fermat's Little Theorem we know that

$$a^{18} \equiv 1 \pmod{19}.$$

Thus

$$a^{1729} \equiv a^{18\cdot 96+1} \equiv (a^{18})^{96} \cdot a \equiv 1^{96} \cdot a \equiv a \pmod{19}.$$

This proves Congruence 11.

Question 12:

Using Fermats little theorem, describe an algorithm that can sometimes detect whether a large integer (say, of 100 or 200 digits) is composite. It is important that your algorithm be more practical than, say, trial division which would run for well over a billion years on a very fast computer with a number of this size!

Solution:

Given a large integer n, we pick a random a with $1 < a < n$ and compute $a^{n-1} \pmod{n}$. If $a^{n-1} \not\equiv 1 \pmod{n}$, then n cannot be prime by Fermat's Little theorem. Note that we can efficiently compute $a^{n-1} \pmod{n}$ using a repeated squaring algorithm: compute a^{2^k} for values of k with $2^k < n-1$ and reconstruct a^{n-1} using the binary expansion of $n-1$.

Additional Remark: We can ask how likely we are to find an a that reveals the compositeness of n. Given a composite n, there certainly exist values of a so that $a^{n-1} \not\equiv 1 \pmod{n}$: we can take any a with $\gcd(a, n) \neq 1$. But such values may be exceedingly rare: if $n = pq$ is a product of two large primes then the probability of randomly hitting a with $\gcd(a, n) \neq 1$ is $\frac{1}{p} + \frac{1}{q}$.

In fact, there exist composite numbers, called Carmichael numbers, so that for any a with $\gcd(a, n) = 1$ and $1 < a < n$ we have $a^{n-1} \equiv 1 \pmod{n}$. The smallest example is $561 = 3 \cdot 11 \cdot 17$. A large Carmichael number will defeat the primality test described above with high probability. While rare, Carmichael numbers aren't that rare: the number of Carmichael less than x is at least $x^{2/7}$.

A better algorithm is described in the next problem.

Question 13:

Show that if p is prime, and $\gcd(a,p)=1$, then $a^{(p-1)/2}=1$ or $-1 \pmod p$. Show that this statement ceases to be true when $p=1729$. More generally, show that if $p-1=2^r m$ with m odd, the sequence $(a^{p-1}, a^{\frac{p-1}{2}}, a^{\frac{p-1}{4}}, \ldots, a^{\frac{p-1}{2^r}})$ (taken modulo p) starts off with a sequence of 1's and that the first term that differs from 1 is equal to -1. This remark is the basis for the Miller-Rabin primality test which is widely used in practice.

Solution:

1. There first term of the sequence starts off with a 1 since $a^{p-1} \equiv 1 \pmod p$.
2. Let $t = a^{(p-1)/2} \pmod p$. We know that $t^2 \equiv a^{p-1} \equiv 1 \pmod p$. By Exercise 7 we must have $t=1$ or $t=-1$. So the second term in the sequence is ± 1.
3. Suppose that $a^{(p-1)/2} \equiv 1 \pmod p$ then again by Exercise 7 we find $a^{(p-1)/4} \equiv 1 \pmod p$ or $a^{(p-1)/4} \equiv -1 \pmod p$. This means that if the second term in the sequence is 1 then the third term in the sequence is ± 1.
4. Continuing we find the sequence starts off with a sequence of 1's and the first term that differs form 1 is equal to -1.

Note that $p=1729$ is not prime; in fact 7 divides 1729. So 7^{1728} can't possibly be congruent to 1 or -1, since it must be divisible by 7. Hence the sequence $(a^{p-1}, a^{\frac{p-1}{2}}, ...)$ does not start with a ± 1.

Additional Remark 1: The Miller-Rabin test works as follows. Write $p-1=2^h \cdot k$ for a positive integer h and an odd integer k. Suppose that $1<a<p$ and $a^{2^m \cdot k}=1$ for some m with $1 \le m \le h$. Then $a^{2^{m-1} \cdot k}$ must be 1 or -1 by the reasoning given above. So to test p for primality, we choose such a random a and compute $a^k, a^{2k}, \ldots, a^{2^h \cdot k}$. If we ever progress to 1 from something other than 1, we know that p can't be prime.

For example, for 1729, choose $a=2$. Note that $1728 = 2^6 \cdot 3^3$. So we compute

$$\begin{aligned} 2^{27} &\equiv 645 \pmod{1729} \\ 2^{54} &\equiv 1065 \pmod{1729} \\ 2^{108} &\equiv 1 \pmod{1729} \end{aligned}$$

So 1729 can't be prime, since $1065^2 \equiv 1 \pmod{1729}$. You can think about the Miller-Rabin test as an efficient method to generate such contradictions.

Additional Remark 2: Note that the probability of finding such an a is much higher than the probability of finding an a that fails the primality test given in the previous problem. In fact, 1729 is a Carmichael number, but our first choice of a showed its compositeness using the Miller-Rabin test. It can be shown that for a fixed odd n, the probability of a randomly chosen a proving the compositeness of n via the Miller-Rabin Test is at least 3/4.