② a) Given: $(\mathbb{Z}/p^k\mathbb{Z})^*$, $p>2$, $k \geq 1$, p-prime

Prove: $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic

Proof:

Base: We know that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, so we have a generator g of order $p-1$. If $(\mathbb{Z}/p^2\mathbb{Z})^*$ is to be cyclic, g must be of order $p(p-1)$ in $(\mathbb{Z}/p^2\mathbb{Z})^2$.

If g has order $|\langle g \rangle|$ in $(\mathbb{Z}/p^2\mathbb{Z})^*$, then $|\langle g \rangle|$ divides $|(\mathbb{Z}/p^2\mathbb{Z})^*| = p(p-1)$. Furthermore $g^{|\langle g \rangle|} \equiv 1 \pmod{p}$, which means $p-1 \mid |\langle g \rangle|$, which in turns yields $|\langle g \rangle| = p-1$ or $|\langle g \rangle| = p(p-1)$.

In the general case, we would like to prove that for $k \geq 2$, if g' is a generator of $(\mathbb{Z}/p^k\mathbb{Z})^*$, then g' is also a generator of $(\mathbb{Z}/p^{k+1})^*$. Since we have seen that there exist a generator $g' = g$ when $k=2$, by induction we can prove that g' is a generator for all $k \geq 2$.

If we consider the ~~Lemma~~ Lemma: I

For any X and $k \geq 1$,

$x^p \equiv 1 \mod p^{k+1} \iff x \equiv 1 \mod p^k$

Ind: Suppose that g' has order $|(\mathbb{Z}/p^k\mathbb{Z})^*| = p^{k-1}(p-1)$ in $(\mathbb{Z}/p^k\mathbb{Z})^*$. As when we considered $k=2$, we can again see that $|\langle g \rangle|$ in $(\mathbb{Z}/p^{k+1}\mathbb{Z})^*$ is either $p^k(p-1)$ or $p^{k-1}(p-1)$.

Continue on next page →

② a)

When $|\langle g' \rangle| \left(\text{in } (\mathbb{Z}/p^{k+1})^*\right) = p^k(p-1)$,

g' is indeed a generator of $(\mathbb{Z}/p^{k+1}\mathbb{Z})^*$ by definition.

For $|\langle g' \rangle| = p^{k-1}(p-1)$, in Lemma I, setting $x = g'^{p^{k-2}(p-1)}$ gives $g'^{p^{k-2}(p-1)} \equiv 1 \bmod p^k$, which contradicts the assumptions we made about the order of g'. This means that the case when $|\langle g' \rangle| = p^{k-1}(p-1)$ is not possible, and therfore the proposition is proven. We only need to prove Lemma I for the above to hold.

Proof of Lemma I:

Base: If $x^p \equiv 1 \bmod p^{k+1}$ or $x \equiv 1 \bmod p^k$, then p divides

$$x^{p-1} + x^{p-2} + \dots + x^{p-p} = \frac{x^p - 1}{x-1}$$

since $x \equiv x^p \bmod p$, $x \equiv 1 \bmod p$. This means that in case $p^k | x-1$ then $p^{k+1} | x^p - 1$.

Ind: Suppose $k \geq 1$ and if $p^{k+1} | x^p - 1$ then $p^k | x-1$. For $k+1$, suppose $p^{k+2} | x^p - 1$ and also $p^{k+1} | x^p - 1$. $x-1$ should therefore be divisible by p^k, $x = 1 + ip^k$ for some integer i. Expanding this gives us

$$x^p = (1 + ip^{k+1}) \bmod p^{k+2}$$

Continue on next page →

② a)

Since $p^{k+2} \mid x^p - 1$, we have $p \mid i$, and $x - 1 = ip^k$, so

$p^{k+1} \mid ip^k$, thus proving the Lemma

~~$(\mathbb{Z}/4\mathbb{Z})^*$ and $(\mathbb{Z}/8\mathbb{Z})^*$ are of the form $(\mathbb{Z}/p^k\mathbb{Z})^*$ with $p=2$ and $k=2$ and $k=3$ respectively.~~

Checking whether a group is cyclic can be done by checking the order of the group and the order of each of its elements. If the order of ≥ 1 element(s) $\neq 1$ is equal to the order of the group, then it is cyclic

For $(\mathbb{Z}/4\mathbb{Z})^*$ we have $|(\mathbb{Z}/4\mathbb{Z})^*| = 2$

$$U(4) = \{1, 3\}$$

checking $3^2 = 1 \bmod 4 =$

$|3| = 2$, so $(\mathbb{Z}/4\mathbb{Z})^*$ is cyclic

For $(\mathbb{Z}/8\mathbb{Z})^*$ we have $|(\mathbb{Z}/8\mathbb{Z})^*| = 4$

$$U(8) = \{1, 3, 5, 7\}$$

$$3^2 = 1 \bmod 8$$

$$5^2 = 1 \bmod 8$$

$$7^2 = 1 \bmod 8$$

None of the elements ~~have a~~ satify the condition so $(\mathbb{Z}/8\mathbb{Z})^*$ is not cyclic. (all order is 2 but we need 4)

② b) Given: n - Carmichael number

~~Pr~~ Prove: $p^2 \nmid n$

~~Given: If n is a Carmichael number, $p^2 \nmid n$~~

Proof:

Suppose $p^2 | n$. Let n' be the product of all primes dividing n. Let g be a generator modulo p^2, such that $g^{p(p-1)} \equiv 1 \mod p^2$. As defined in CRT, an integer b exists which satisfies $b \equiv 1 \mod n'$ and $b \equiv g \mod p^2$. ~~Thus~~ We observe that b is also a generator modulo p^2, and therefore satifies $\gcd(b, n) = 1$, since it is not divisible by p or any element in the set of primes dividing n.

We propose that n is not a pseudoprime to b. From FLT, we have $b^{n-1} \equiv 1 \mod n$, which if holds, we have $b^{n-1} \equiv 1 \mod p^2$ since $p^2 | n$. In this case we have $p(p-1) | n-1$, as $p(p-1)$ is the order of b modulo p^2. Since $p | n$, we have $n-1 \equiv -1 \mod p$, hence $p(p-1) \nmid n-1$.

The contradiction proves that n is not a pseudoprime to the base b.

② c) ~~Prove~~

Given: n - squarefree number

Prove: n is a Carmichael number iff $p-1 \mid n-1$ for every prime divisor p of n

Proof:

Suppose $p-1 \mid n-1$ for $\forall p \mid n$. Take b be a base such that $\gcd(b,n)=1$. We have for $\forall p \mid n$, b^{n-1} is a power of b^{p-1}, so $b^{n-1} \equiv 1 \bmod p$. So, $b^{n-1}-1$ is divisible by all prime factors p of n and their product (n). This makes FLT hold for all bases b. Oppositely, assume there is a p such that $p-1 \nmid n-1$. Let g be a generator modulo p. We must then find b satisfying $b \equiv 1 \bmod \frac{n}{p}$ and $b \equiv g \bmod p$. Then we have $\gcd(b,n)=1$, $b^{n-1} \equiv g^{n-1} \bmod p$. Since $n-1$ is not divisible by the order $p-1$ of g, $g^{n-1} \not\equiv 1 \bmod p$. It follows that $b^{n-1} \not\equiv 1 \bmod p$, which means FLT does not hold. Hence, the proposition holds.

② d) Given: n - Carmichael number

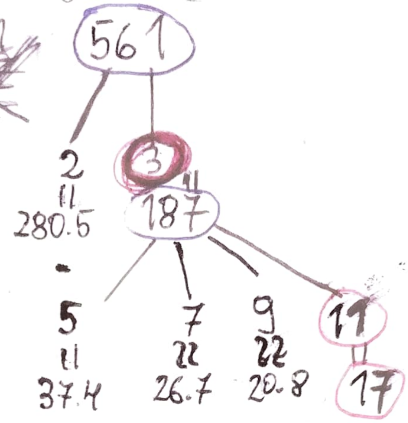
Prove: n must be the product of at least three distinct primes

Proof:

From the proof presented in b) we know that a Carmichael number must be a product of distinct primes. So, it is sufficient to show that the number n is not the product of two distinct primes. Take $n = pq$ and assume $p < q$. If n is a Carmichael number, $n-1 \equiv 0 \mod q-1$ which we know from the proof presented in c). We have $n-1 = p(q-1+1) - 1 \equiv p-1 \mod q-1$ and having $0 < p-1 < q-1$, we see that $p-1 \mod q-1 \not\equiv 0 \mod q-1$, which means n cannot be a product of two primes, thus concluding the proof.

② e) Check 561 is a Carmichael number

Start by dividing 561 by the first members of the ~~prime~~ set of primes until we get an integer as a result and continue until we get 1/~~a~~ known prime



We have $561 = 3 \times 11 \times 17$, so 561 is indeed a Carmichael number

~~To find the next Carmichael number, we may try to increment each of the primes and test whether the resulting number is a Carmichael number.~~

To find the next Carmichael number, it would be tedious to ~~do~~ do it by hand, so we can ~~use a~~ instead use a computer program with the following pseudocode:

~~next := 0~~
~~n := 561~~
~~while next = 0~~ do
~~n := n+1~~
~~for b = 2~~

~~next := 0~~
~~n := 561~~
~~while next = 0 do~~
~~n := n+1~~
~~for b = 2, ...~~

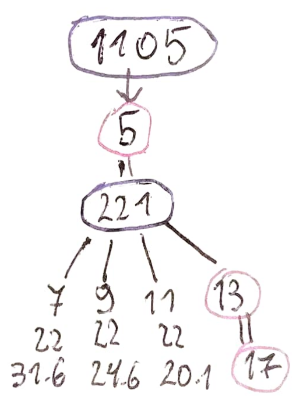
Continued on next page →

② e)

```
next := 0
n := 561
while next = 0 do:
    n := n+1
    if isprime(n) then
        continue
    end if
    next := n
    for b = 2, ..., n-1 do
        if gcd(b,n) = 1 then
            if b^(n-1) mod n ≠ 1 then
                next := 0
                break
            end if
        end if
    end for
end while
return next
```

Implementing the code above returns the number 1105

Finding its prime factors we have:



So the next Carmichael number is $5 \times 13 \times 17 = 1105$

5 b)

Since now we have a number which is only probably prime, there is still a chance it is not. We are able to check whether a number n is prime deterministically in $O(2^{\|n\|/2})$ where $\|n\|$ is the number of bits in n. So this would be highly impossible (only feasible for small numbers). So instead we could use the AKS algorithm, which is deterministic and will gives us the answer in polynomial time.

Another option, assuming GRH holds, is to use a deterministic version of the Miller-Rabin algorithm. From GRH we know that every composite number n has a Miller-Rabin witness a, such that $a \leq 2(\ln n)^2$. So the problem will be reduced to checking all possible witnesses from 2 to $2(\ln n)^2$. This yields a polynomial-time deterministic algorithm, which is feasible to compute.

In conclusion, we can proove that the generated number is prime if we test it using AKS, or in the case GRH holds, using the determinstic version of Miller-Rabin.