7. Show that there is a p such that if $1000 \le m \le 1000000$ then m-prime $\Leftrightarrow \gcd(p,m)=1$

"$\Rightarrow$"

m-prime $\Rightarrow \gcd(p,m)=1$ (1) $[p \neq m]$

Contrapositon: $\gcd(p,m) \neq 1 \Rightarrow m$ is not prime

We assume: $\gcd(p,m) = t \Rightarrow t \mid m$

↳ contradiction with m-prime

$\Rightarrow$ (1) is true

"$\Leftarrow$" if $1000 \le m \le 1000\,000$ there exists p such that $\gcd(p,m)=1 \Rightarrow m$-prime

fundam. th. of arit.

idea: any number that is not prime has an unique factorisation of primes (1),
If p is the product of all primes up to $\sqrt{m}$, then we know, for sure that if $\gcd(p,m)=1$ then m must be prime ! (2)

why?

euclid's lemma

(1)

Theorem of prime factorisation: $\forall m > 1$ integer, m has a unique prime factorisation.

- Every integer $m>1$ is a product of prime numbers

Suppose this is false. Then there has to be an integer $m > 1$ that is not equal to a product of primes $\left.\right\}$ m-not prime $\Rightarrow$ m-composite $\Rightarrow \exists a,b$ such that $m = ab$, $1<a<m$, $1<b<m$.

Let's assume m is the smallest possible int that is not a product of pr's.

⇓

a and b are prod. of primes, but $m=ab$ $\Rightarrow$ m has to be a product of primes.

- uniqueness

two different factorisations

Smallest integer with two factorisations $\rightarrow m = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_l$

for $k=1$, $l=1$ proof is trivial

$l, k \ge 2$,

euclid's lemma

Let r be the largest from (q_l, p_k) (assume q_l) $\Rightarrow r \mid m \Rightarrow p_1 p_2 \cdots p_k \vdots r \Rightarrow$ at least one p is divisible by r

But $p_1 \le p_2 \cdots \le p_k$ and $p_k \le q_l = r \Rightarrow p_k = r$

Similarly, $r = q_l$

But this is not possible because $\frac{m}{r}$ is an integer $< m$ with two different prime factorisations. (contradiction because we assumed m to be the smallest such integer) (with two factorisations)

(27) Why do we only check to $\sqrt{n}$ to see if n is prime?

If n is not prime, then: $n = a \cdot b$.

a and b can't be both $> \sqrt{n}$

if $a \le b$ then $a^2 \le ab = n$

So, in any factorisation of n we find a factor smaller than $\sqrt{n}$.

For our problem:

if p is the product of all primes up to the $\sqrt{n}$ then if n is not prime we will surely find a prime divisor of n in the factorsation of p.

Let $p = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where $p_1, p_2, \ldots p_k$ are primes $< \sqrt{n}$.

if $\gcd(n,p) = 1 \overset{?}{\Rightarrow} n$ - prime

Assume n - is not prime

We have to prove that $\gcd(n,p) \neq 1$

n - not prime $\Rightarrow$ it has a unique factoisation: $n = n_1 \cdot n_2 \cdot \ldots \cdot n_l$

if the $\gcd(n,p) = 1$ then n and p have no common divisors (are coprime), but if n_1 is the smallest prime such that $n_1 | n$, then $n_1 < \sqrt{n} \Rightarrow n_1 | p$ which is a contradiction.

So, if n and p are coprime n can't have divisors other than 1 and n itself.

```python
def product():
    r=1
    for i in range (1,1000):
        if is_prime(i):
            r*=i
    return r


print(product())
```

product() › for i in range (1,1000) › if is_prime(i)

main

```
C:\TheNumber\venv\Scripts\python.exe C:/TheNumber/main.py
195903406449990834312625081982063810461239723905893682238826053289686663163798706618
 51951648789482321596229559115436019149189529725215266728292282990852649023362731392
 4040179391420109582613936349594714837571967216722434100671185162276611331351924888 4
 898991489215718830867989687513743951933890396809490554975038640710603383658666068 35
 392010116359179000399044950652032997495429859931346698148053184740805812078911259 10

Process finished with exit code 0
```