2 prime

$\binom{p}{k}p^k \qquad 0<k<p$

$$(1+p)^p = \sum_{k=0}^{p}\binom{p}{k}p^k = 1 + \binom{p}{1}p + \binom{p}{2}p^2 + \cdots + \binom{p}{p-1}p^{p-1} + p^p$$

$p \quad p \quad p \quad p \quad p \quad p \quad p^2$

---

$S = \{n \in \mathbb{N} \mid a^n \text{ and } a \text{ have same units digit for all } a\}$

$a = 2 \qquad a = 3$

$a^2 = 4$

$a^3 = 8$

$a^4 = 16$

$a^5 = 32$

$a^6 = 64$

$a^7 = 128$

$a^8 = 256$

$a^9 = 512$

$a^n$ and $a$ have same units digit is equivalent to $a^n \equiv a \pmod{10}$

---

$\#\{k=1,\dots,n \mid \gcd(k,n)=d\}$ $\qquad$ $d$ fixed divisor of $n$.

$\varphi(n/d) = \#\{\ell=1,\dots,n/d \mid \gcd(\ell,n/d)=1\}$

$$\gcd(k,n)=d \iff \gcd(d\cdot k/d,\, d\cdot n/d)=d \overset{(2.7)}{\iff} d\cdot\gcd(k/d,n/d)=d \qquad (*)$$

$$\iff \gcd(k/d,n/d)=1.$$

$S_d = \{k = 1, \dots, n \mid \gcd(k,n) = d\}$ $\{l = 1, \dots, n/d \mid \gcd(l, n/d) = 1\}$

$k \longmapsto k/d$

$ld \longleftarrow l$

sets are in "1-1 correspondence" so must have same number of elements.

---

- number div by $1, 2, \dots, 12$
- square
- 8-digits

} only 2 possibilities!

---

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod a$$
$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod b$$

$$a^{\varphi(a)} + b^{\varphi(b)} \equiv 1 \pmod{ab}$$

① Prove the (mod a) & (mod b) congruences using Euler's thm.

② Deduce the (mod ab) congruence.

CRT

$x \equiv 1 \pmod a$
$x \equiv 1 \pmod b$

since $\gcd(a,b) = 1$, this system has a unique solution mod ab.

$x = 1$ is a solution, but so is $x = a^{\varphi(b)} + b^{\varphi(a)}$.

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$$

Cor 2 to thm 2.4

$a \mid (a^{\varphi(b)} + b^{\varphi(a)} - 1)$
$b \mid (a^{\varphi(b)} + b^{\varphi(a)} - 1)$

since $\gcd(a,b) = 1$,

$\rightsquigarrow ab \mid (\dots)$

---

$n = 6$

LHS $\gcd(1,6) + \gcd(2,6) + \gcd(3,6) + \gcd(4,6) + \gcd(5,6) + \gcd(6,6)$

1 2 3 2 1 6

| RHS | | | | |
|---|---|---|---|---|
| $d$ | 1 | 2 | 3 | 6 |
| $6/d$ | 6 | 3 | 2 | 1 |
| $\varphi(6/d)$ | 2 | 2 | 1 | 1 |

$$\sum d\,\varphi(n/d) = 1\cdot 2 + 2\cdot 2 + 3\cdot 1 + 6\cdot 1$$

$$S_d = \{k=1,\dots,n \mid \gcd(k,n)=d\}$$

$$\sum_{k=1}^{n} \gcd(k,n) = \sum_{d\mid n} d\cdot \underbrace{\#S_d}_{\substack{\downarrow \text{ by earlier} \\ \varphi(n/d)}}$$

---

$$(p+1)^p = \underbrace{p^p + \binom{p}{1}p^{p-1} + \binom{p}{2}p^{p-2} + \dots + \binom{p}{p-2}p^2}_{\substack{\text{div by } p^2 \text{ since } \binom{p}{k}p^{p-k} \\ \text{where } p-k \geq 2.}} + \underbrace{\binom{p}{p-1}p}_{\uparrow} + 1$$

---

$$n = (d_m d_{m-1} \cdots d_0)_p$$
$$= d_m p^m + d_{m-1}p^{m-1} + \dots + d_1 p + d_0$$

$$x^{n+m} = x^n x^m$$

$$a^n = a^{d_m p^m + \dots + d_1 p + d_0}$$
$$= a^{d_m p^m} \cdots\cdots a^{d_1 p} a^{d_0}$$

$$\left[ x^{p^m} \equiv x \bmod p \text{ for any } m. \right]$$

$$a^{d_m + \dots + d_0} = a^{d_m} \cdots\cdots a^{d_1} a^{d_0}$$

$$a^{d_1 p} = (a^{d_1})^p \equiv a^{d_1} \mod p$$
$$a^{d_2 p^2} = ((a^{d_2})^p)^p \equiv (a^{d_2})^p \equiv a^{d_2} \mod p$$

$$27 = 1\cdot 16 + 9$$

$$= (19)_{16}$$

$$16 = 2^4$$

$$29 = 1\cdot 16 + 11$$

$$= (1B)_{16}$$

---

WTS: $\displaystyle\sum_{k=1}^{n} \gcd(k,n) = \sum_{d\mid n} d\cdot\varphi(n/d)$

Let $S_d = \{k=1,\dots,n \mid \gcd(k,n)=d\}$. For each $k\in S_d$, $\gcd(k,n)=d$, so in the sum on the LHS there are $\#S_d$ $d$'s being added together for each divisor $d$ of $n$, ie,

$$\sum_{k=1}^{n} \gcd(k,n) = \sum_{d\mid n} d\cdot \# S_d.$$

So it is sufficient to show that $\#S_d = \varphi(n/d)$.

By definition, $\varphi(n/d) = \#\{\ell=1,\dots,n/d \mid \gcd(\ell,n/d)=1\}$. so, to show that $\#S_d = \varphi(n/d)$, we need to show that the sets

$$S_d = \{k=1,\dots,n \mid \gcd(k,n)=d\} \quad \& \quad \{\ell=1,\dots,n/d \mid \gcd(\ell,n/d)=1\}$$

are in 1-1 correspondence.

---

$h = 1, 2, \dots$

$a$ is a primitive root of 19.

Your list should have the property that, no matter what primitive root I choose for $a$,

$$a \equiv 3^h \pmod{19}$$

for some $h$ in your list.

$$2 \equiv 3^7 \pmod{19}.$$

1. Show $n = (2p_1 \cdots p_r)^4 + 1$ has an odd prime divisor p.

2. p is not in list $p_1, \dots, p_r$.

3. From (a), $p \equiv 1 \mod 8$.

---

| | |
|---|---|
| $3^1 \equiv 3$ | $2^1 \equiv 2$ |
| $3^2 \equiv 9$ | $2^2 \equiv 4$ |
| $3^3 \equiv 8$ | $2^3 \equiv 8$ |
| $3^6 \equiv$ | $2^6 \equiv$ |
| $3^9 \equiv$ | $2^9 \equiv$ |
| $3^{18} \equiv 1$ | $2^{18} \equiv 1$ |

---

- $k$ is order of $x$. $\Rightarrow k \mid \varphi(p)$

$x^3 \equiv 1 \pmod p$

what is the order of $x$?

$x^1 \equiv 1 \pmod p \Rightarrow x^3 \equiv 1 \pmod p$ ⇝ order 1.

"always a cube root"

Suppose $x \not\equiv 1 \pmod p$ but $x^3 \equiv 1 \pmod p$.

$x^2 \equiv 1 \pmod p. \Rightarrow x^3 \equiv x \not\equiv 1 \pmod p.$

So $x$ can't have order 2, so it must have order 3.

so $3 \mid p-1$

If 1 has a nontrivial cube root, then $p \equiv 1 \pmod 3$.

For converse:

- If 1 doesn't have a nontrivial cube root...
- If $p \equiv 1 \pmod 3$ . . .