Power Remainders, Euler's Theorem

D

All letters will denote natural numbers or zero.
The absolute value sign, $|\ |$ will denote the remainder to a fixed d divider.
The b , b^2, b^3, . . sequence is called a power sequence and we'll regard the remainders of these, that is $r_1 = |b|$, $r_2 = |b^2|$, $r_3 = |b^3|$, . . These are very useful.
Indeed, $|b^{n+1}| = ||b^n||b||$ and so we can establish quite easily the remainder of a huge power by merely calculating with small numbers. But beside this practicality these remainder sequences have amazing regularities and we'll prove one such law.
The most important special remainder is 0 that is dividability, denoted as $d \mid a$.
Its negative will be denoted as $d \neg\mid a$.
The c common dividers of two a , b numbers are especially important and if such c can only be 1, that is $c \mid b , d \rightarrow c = 1$ then we call a , b as relative primes.

T

1. $d \mid b \rightarrow$ our sequence is all 0.
2. $d \neg\mid b \rightarrow$ our sequence has no 0 in it.
3. $c \mid b , d \rightarrow$ c divides all members of our sequence.
4. 1 occurs in our sequence $\leftrightarrow$ b , d are relative primes.

P

$r_n = (b^n - kd)$'s smallest possible value and so:

1. $b = md \rightarrow b^n = Md \rightarrow r_n = 0$ at $k = M$.
2. $b \neq md \rightarrow b^n \neq Md \rightarrow r_n \neq 0$ at any k.
3. $c \mid b , d \rightarrow$ c divides $b^n - kd$.
4. By 3. $c \mid b , d$ and $c > 1 \rightarrow$ we can't have an occurring 1.
   So we must show that: b , d are relative primes $\rightarrow$ for some m, $|b^m| = 1$.
   Let's regard a $|b^N|$ that has same value as an earlier $|b^n|$.
   This must happen since the possible remainders are finite many.
   $|b^N| = |b^n| \rightarrow b^N - b^n = b^n(b^{N-n} - 1) = kd$.
   By Euclid's Lemma since b , d are relative primes d must divide $b^{N-n} - 1$.
   Thus $|b^{N-n}| = 1$.

D

The place of the first appearing 1 value is $\mu(b , d)$ or in short μ.

T

There can be no returning values before μ.

P

Suppose that an $N < \mu$ place remainder would return to an even earlier n, that is:
$|b^N| = |b^n|$ were with $n < N < \mu$.
We get again that $b^N - b^n = b^n(b^{N-n} - 1) = kd$ were.
And so $|b^{N-n}| = 1$ were too, contradicting that μ is the first 1 occurring place.

T

Euler's Theorem:
If b , d are relative primes and there are $\varphi(d)$ many smaller than d numbers that are relative primes with d, then at $\varphi(d)$ we have a 1. So $|b^{\varphi(d)}| = 1$.

R Since after an occurring 1 everything repeats, it would be enough to show that μ divides $\varphi(d)$ that is $\varphi(d) = k\mu$. Or even formally, from assuming $\varphi(d) = k\mu$:
$|b^{\mu}| = 1 \rightarrow |b^{\varphi(d)}| = |b^{k\mu}| = ||b^{\mu}|^{k}| = 1.$

The $r_1 = |b|, r_2 = |b^2|, r_3 = |b^3|, \ldots, r_{\mu} = |b^{\mu}| = 1$ initial remainder set is a subset of the $\Phi(d)$ set of all s numbers under d that are relative primes with d.
Indeed, $r_n = b^n - kd$ and so if a $c > 1$ divider of d would divide r_n then c would have to divide b^n and thus b too, contradicting what we assumed about b , d.

But of course not all members of $\Phi(d)$ can become remainders if $\mu < \varphi(d)$.
So we might expect that the $r_1, r_2, \ldots, r_{\mu} = 1$ initial segment is some special subset of $\Phi(d)$ relating to the outside ones, that is to $\Phi(d) - \{ r_1, \ldots, r_{\mu} \}$ so that these form some disjoint similar groups. Then it would follow that μ divides $\varphi(d)$.
This expectation is true but its proof is difficult.
So instead we'll regard the full $\Phi(d)$ set itself and apply a trick.

P Let $\Phi(d) = \{ s_1, s_2, \ldots, s_{\varphi(d)} \}$.
Let $b\Phi(d)$ abbreviate $\{ bs_1, bs_2, \ldots, bs_{\varphi(d)} \}$ and let
$|b\Phi(d)|$ abbreviate $\{ |bs_1|, |bs_2|, \ldots, |bs_{\varphi(d)}| \}$.

We claim that $|b\Phi(d)| = \Phi(d)$. Indeed, as easy to see, all members of $|b\Phi(d)|$ are from $\Phi(d)$ and they are all different so they must exhaust the full $\Phi(d)$.

Now let's form the remainders of the total product of our two equal sets.

$$|\Pi\,|b\Phi(d)|| = |\Pi\,\Phi(d)|$$

$$|bs_1\, bs_2 \ldots bs_{\varphi(d)}| = |s_1\, s_2 \ldots s_{\varphi(d)}|$$

$$|b^{\varphi(d)}\, s_1\, s_2 \ldots s_{\varphi(d)}| = |s_1\, s_2 \ldots s_{\varphi(d)}|$$

So $|A\,B| = |B|$

Which might suggest that $|B| = 0$ or $|A| = 1$.

But this is not true as $A = 6, B = 4$ shows with $d = 10$ since $|6x4| = |24| = |4|$.

Luckily B , d being relative primes already implies that $|A| = 1$ with using again Euclid's Lemma.
Indeed, $|A\,B| = |B| \rightarrow$ d divides $A\,B - B = B(A - 1)$ so d divides $A - 1$.

R The theorem doesn't reveal the full picture about $\mu(b, d)$. But observe that:
If d is a prime then $\varphi(d) = d - 1$ and if d is a composite then $\varphi(d) < d - 1$.
Also observe that even if d is a prime, μ can be smaller than $d - 1$.
For example, with the simplest $b = 2$ base with the $d = 7$ prime divider: $|2^3| = 1$.
So $\mu(2, 7) = 3 < \varphi(7) = 6$. Not surprisingly though 3 divides 6.

The ancient Chinese mathematicians realized that $|2^{d-1}| = 1$ with d being a prime. They also falsely believed that for composite d this can not be true.
So they believed this law to be a primality test.
Fermat discovered the generalization $|b^{d-1}| = 1$ with b not being a multiple of the d prime divider. Euler's above theorem of course gives this instantly because b not being a multiple of d means that b, d are relative primes and $d - 1 = \varphi(d)$.
Fermat's generalization as generalized primality test is trivially false and for example using base 4 we have the composite $d = 15$ with which:
$|4^{15-1}| = |(4^2)^7| = ||4^2|^7| = 1$.
The smaller 3 base needs a more complicated $d = 91 = 7 \cdot 13$ counter example:
$|3^{91-1}| = |(3^6)^{15}| = ||3^6|^{15}| = 1$ because $3^6 = 729 = 8 \cdot 91 + 1$.
The smallest 2 base needs the most complicated $d = 341 = 11 \cdot 31$:
$|2^{341-1}| = |(2^{10})^{34}| = ||2^{10}|^{34}| = 1$ because $2^{10} = 1024 = 3 \cdot 341 + 1$.
Actually, this was not recognized by Euler, neither the general fact that all b bases have some d composite cases satisfying Fermat's equation.
But something even more surprising is true too! Namely, that there are d composites that satisfy Fermat's equation for all b bases that are relative primes with d.
The first such is only 561 and this was missed by Gauss just as 341 was by Euler.
Of course, the more important question was that we started this remark too about μ.
Euler knew by his theorem that if d is composite then for any b base there is an earlier 1 place than $d - 1$, because then $\varphi(d) < d - 1$. More importantly, he also knew without a proof that if d is a prime then there is always some b base that forbids such early 1 occurrence and called these b-s as primitive roots of d.
Gauss kept this name and proved their existence. But he still didn't realize that the duality of d being a prime or not, corresponding exactly to an existence or non existence of b that forbids early μ place of 1 offers a primality test.
Lucas worked out this first usable primality test.