FlT, Euler's Totient, and Orders

David Tang

October 2019

1 Fermat's Little Theorem

Fermat's Little Theorem, or FlT, states that, for any prime p and natural number a, $a^{p-1} \equiv 1 \pmod{p}$. To account for the a divides p case, we can reword it as, for any prime p and integer a, $a^p \equiv a \pmod{p}$. Euler proved this using induction. First, we prove the base case, $a = 0$. This is true as $0 \equiv 0 \pmod{p}$.

Now for induction, we seek to prove it for the $k+1$ case given the k case. By Binomial Theorem, we know that $(k+1)^p = \sum_{i=0}^{p} \binom{p}{i} k^i$. Since $\binom{p}{i} \equiv 0 \pmod{p}$ for all $i \neq 0, p$. Thus, we have that $(k+1)^p \equiv k^p + 1 \equiv k + 1 \pmod{p}$.

2 Euler's Totient Theorem

Euler's Totient Theorem is a generalization of Fermat's Little Theorem. It states that, if a is relatively prime to m, then $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(m)$ is the number of integers from 1 to m that are relatively prime to m. We may prove this as follows:

Let $r_1, r_2, \cdots, r_{\phi(m)}$ represent the integers from 1 to m that are relatively prime to m. Then for each i, ar_i also represents a residue that is relatively prime to m, modulo m. Furthermore, since a is relatively prime to m, $ar_i \equiv ar_j \pmod{m}$ if and only if $r_i \equiv r_j \pmod{m}$. Hence, $ar_1, ar_2, \cdots, ar_{\phi(m)}$ also represent the distinct residues that are relatively prime to m, modulo m. Therefore, $(ar_1)(ar_2)\cdots(ar_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$ Cancelling $r_1 r_2 \cdots r_{\phi(m)}$ on both sides, we get $a^{\phi(m)} \equiv 1 \pmod{m}$.

3 Wilson's Theorem

This theorem states that $(p-1)! \equiv -1 \pmod{p}$. The proof starts by supposing p is a prime. Then each of the integers $1, \ldots, p-1$ has an inverse modulo p. The inverse exists because $\frac{1}{a} \equiv a^{p-2} \pmod{p}$. This inverse is unique, and each number is the inverse of its inverse. If one integer a is its own inverse, then

$$0 \equiv a^2 - 1 \equiv (a-1)(a+1) \pmod{p},$$

so that $a \equiv 1$ or $a \equiv p-1$. Thus we can partition the set $\{2, \ldots, p-2\}$ into pairs $\{a, b\}$ such that $ab \equiv 1 \pmod{p}$. It follows that $(p-1)$ is the product of these pairs times $1 \cdot (-1)$. Since the product of each pair is conguent to 1 modulo p, we have

$$(p-1)! \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}.$$

4 Orders

Euler's Theorem proves that there exist positive integers n such that $a^n \equiv 1 \pmod{m}$. Let d be the smallest positive integer such that $a^d \equiv 1 \pmod{m}$. Then we say that d is the order of a modulo m, denoted by $\text{ord}_m(a)$, or simply $\text{ord}(a)$ if the modulus m is understood.

An important lemma is: If a is relatively prime to m, then $a^n \equiv 1 \pmod{m}$ if and only if $\text{ord}(a)|n$. Furthermore, $a^{n_1} \equiv a^{n_2} \pmod{m}$ if and only if $\text{ord}(a)|(n_1 - n_2)$.

Proof: Let $d = \text{ord}(a)$. It is clear that if $d|n$, then $a^n \equiv 1 \pmod{m}$. On the other hand, let n be a positive integer such that $a^n \equiv 1 \pmod{m}$. By the Division Algorithm, there exist integers q and r such that $n = qd + r$, $0 \leq r < d$. Then $a^n \equiv a^{qd+r} \equiv (a^d)^q a^r \equiv a^r \pmod{m}$, so $a^r \equiv 1 \pmod{m}$. But $r < d$, so by minimality of d, $r = 0$, which means $d|n$. Then $a^{n_1} \equiv a^{n_2} \pmod{m} \iff a^{n_1 - n_2} \equiv 1 \pmod{m} \iff d|(n_1 - n_2)$.

5 Examples

5.1 First Example

(2019 AIME I Q14) Find the least odd prime factor of $2019^8 + 1$.

5.2 Second Example

(2014 HMMT November General Q10) Suppose that m and n are integers with $1 \leq m \leq 49$ and $n \geq 0$ such that m divides $n^{n+1} + 1$. What is the number of possible values of m?

6 Problems

Point weights are given. Try to get at least $\boxed{25}$ points. Note that sources are NOT given for psychological reasons, although you could also just search them up or ask me.

1. (2) Find the order of 2 modulo 9.
2. (3) Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7$.
3. (3) If $133^5 + 110^5 + 84^5 + 27^5 = n^5$, find the value of n.
4. (3) Let $a_n = 6^n + 8^n$. Determine the remainder on dividing a_{83} by 49.
5. (3) Prove that
$$\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$$
is an integer for all integers n.
6. (4) If $f(x) = x^{x^{x^x}}$, find the last two digits of $f(17) + f(18) + f(19) + f(20)$.
7. (4) Determine all non-negative integral solutions $(n_1, n_2, \ldots, n_{14})$ if any, apart from permutations, of the Diophantine Equation $n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599$.
8. (4) Show that if p is prime, then every prime factor of $2^p - 1$ is greater than p.
9. (4) Show that the equation $(a^3 + (a+1)^3 + \ldots + (a+6)^3 = b^4 + (b+1)^4)$ has no solutions in integers (a, b).
10. (6) Prove that for each positive integer n there exist n consecutive positive integers none of which is an integral power of a prime number.
11. (6) Find the least positive integer n such that when 3^n is written in base 143, its two right-most digits in base 143 are 01.
12. (6) The increasing infinite arithmetic sequence of integers $x_1, x_2, \cdots$ contains the terms 17! and 18!. Compute the greatest integer X for which $X!$ must also appear in the sequence.
13. (6) Find the highest degree k of 1991 for which 1991^k divides the number
$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$
14. (9) Determine all positive integers relatively prime to all the terms of the infinite sequence
$$a_n = 2^n + 3^n + 6^n - 1, \ n \geq 1.$$
15. (9) Find the least positive integer N such that the only values of n such that $1 + N \cdot 2^n$ is a prime are multiples of 12.

7 Solutions to Examples

7.1 First Example

Notice that it's equivalent to finding a prime p such that $2019^8 \equiv -1 \pmod{p}$. Thus, $2019^{16} \equiv 1 \pmod{p}$ so $\text{ord}_p(2019) = 1, 2, 4, 8$, or 16. Since $2019^8 \equiv -1 \pmod{p}$, we get that $\text{ord}_p(2019) = 16$. So $16|p-1$ by Fermat's Little Theorem which implies that $p \equiv 1 \pmod{16}$. Checking the primes, the first two primes that follow this condition is 17 and 97. Bashing, 17 doesn't work but 97 does, so our answer is 97.

7.2 Second Example

If n is even, $n+1|n^{n+1}+1$, so we can cover all odd m.
If m is even and $m|n^{n+1}+1$, then n must be odd, so $n+1$ is even, and m cannot be divisible by 4 since $x^2+1 \equiv 1, 2 \pmod{4}$ or any prime congruent to 3 $\pmod{4}$. The proof of the second statement can be done by contradiction. Assume there exists an integer x such that $x^2+1 \equiv 0 \pmod{p}$ for $p = 4k+3$. Then, $x^{2(2k+1)} \equiv x^{4k+2} \equiv x^{p-1} \equiv 1 \pmod{p}$. But if $x^2 \equiv -1 \pmod{p}$, then $x^{2(2k+1)} \equiv -1 \pmod{p}$ so contradiction.

Conversely, if $\frac{m}{2}$ has all factors 1 $\pmod{4}$, then we seek to prove that there exists $N \equiv 1 \pmod{4}$ such that $m|N^2+1|N^{N+1}+1$ (note $\frac{(N+1)}{2}$ is odd). We can prove this by first proving that $x^2+1 \equiv 0 \pmod{q}$ has a solution for all primes $q \equiv 1 \pmod{4}$. This solution can be explicitly found since $-1 \equiv (p-1)! \equiv 1 \cdots \frac{p-1}{2}\frac{p+1}{2} \cdots (p-1) \equiv ((\frac{p-1}{2})!)^2(-1)^{\frac{p-1}{2}} \equiv ((\frac{p-1}{2})!)^2$. Now, we may see that if $a_1^2 \equiv -1 \pmod{q_1}$, $a_2^2 \equiv -1 \pmod{q_2}$, where $q_1 \equiv q_2 \equiv -1 \pmod{4}$, then we can find an integer b such that $b - a_i \equiv 0 \pmod{q_i}$ for $i = 1, 2$. The only exception would be if q_1 and q_2 share a common factor. But, this can't happen as this common factor must be ≥ 5 and $2 * 5^2 = 50 > m \geq 49$. Then, we find that $b^2 \equiv -1 \pmod{q_i}$ so by CRT, $b^2 \equiv -1 \pmod{q_1 q_2}$. Thus, if we keep on combining the primes, we reach an integer B such that $B^2 + 1 \equiv 0 \pmod{\frac{m}{2}}$. Yet, since we can just add $\frac{m}{2}$, which is odd, to B, we can always make B odd so that $B^2 + 1 \equiv 0 \pmod{2}$. Again, if this new B is not equal to 1 $\pmod{4}$, we can add m to B to make it so, as $B + m \equiv 3 + 2 \equiv 1 \pmod{4}$. This proves our assertion that there exists an N such that $N \equiv 1 \pmod{4}$ and $N^2 + 1 \equiv 0 \pmod{m}$.

So the only bad numbers take the form $2k$, where $1 \leq k \leq 24$ is divisible by at least one of $2, 3, 7, 11, 19, 23, 31, \cdots$. We count $k = 2, 4, \cdots, 24$ (there are 12 numbers here), $k = 3, 9, 15, 21$ (another four), $k = 7, 11, 19, 23$ (another four), giving a final answer of $49 - 12 - 4 - 4 = 29$.