Basic Theorems in Number Theory

1. The Fundamental Theorem of Arithmetic: Any integer greater than 1 can be written as a unique product (up to ordering of the factors) of prime numbers.

eg. $13608 = 2^3 \cdot 3^5 \cdot 7$

2. The remainder theorem: For any positive integers $a \geq b$, we can find unique integers *k* and *r* such that $a = kb + r$, where $0 \leq r < b$.

eg. when dividing 205 by 3, we will have 68 as the divisor and 1 as the remainder, that means: $205 = 68 \times 3 + 1$.

3. Theorem: There are infinitely many primes.

Euclid's Proof: Assume there are finitely many primes: $P_1, P_2, P_3, \ldots, P_n$ in order, i.e. $P_1 < P_2 < P_3 < \ldots < P_n$. Then $k = P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_n + 1$ is an integer bigger than all the assumed primes above, so *k* is a composite. To consider the prime factorization of k, k must have a prime factor from the set of all primes $P = \{P_1, P_2, P_3, \ldots, P\}$, let's name it P_r, where r is from $\{1,2,3,\ldots,n\}$.

$k = P_r \cdot m$, where m is a positive integer;

$P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_n + 1 = P_r \cdot m$;

$1 = P_r \cdot m - P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_r \cdot \ldots \cdot P_n$;

Factor out P_r,

$1 = P_r \cdot (m - P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_{r-1} \cdot P_{r+1} \cdot \ldots \cdot P_n)$;

Let $t = m - P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_{r-1} \cdot P_{r+1} \cdot \ldots \cdot P_n$, then

$1 = P_r \cdot t$.

That tells 1 is a composite number that can be factored into two factors, which contracts the fact 1 is non-factorable.

4. Fermat's Little Theorem: Let *p* be a prime which does not divide the integer *a*, then the remainder of a^{p-1} (when dividing by *p*) is 1.

Proof: Start by listing the first *p*-1 positive multiples of *a*:

$$a, 2a, 3a, \ldots (p-1)a$$

(a) First, let's prove all the above multiples of *a* are not divisible by *p*.

For *ra* to be divisible by *p*, where *r* is a number from the set $\{1,2,3,...,p-1\}$, either *r* or *a* needs to be divisible by *p*. But it is given that *a* is not divisible by *p*, and any number in $\{1,2,3,...,p-1\}$ is not divisible by *p*. That proves *a*, 2*a*, 3*a*, ... (*p* -1)*a* are not divisible by *p*.

(b) Secondly, let's prove the above numbers have different remainder (when dividing by *p*).
If suppose that for any *r* and *s* ($r \neq s$) from the set $\{1,2,3,...,p-1\}$, *ra* and *sa* have same remainder (when dividing by *p*), then *r* and *s* must have same remainder (when dividing by *p*), since *p* does not divide *a*. This contracts that *r* and *s* are two distinct positive integers less than *p*. So *a*, 2*a*, 3*a*, ... (*p* -1)*a* above have distinct remainders (when dividing by *p*) and the remainders can't be *0*, that is, the distinct remainders must be congruent to 1, 2, 3, ..., *p*-1.

(c) Thirdly, let's prove for any integer *k* and *s*, their remainder (when dividing by *p*) are r_1 and r_2, respectively. Then $k \cdot s$ and $r_1 \cdot r_2$ have same remainder (when dividing by *p*).
k has remainder r_1, and s has remainder r_2, so

$$k = k_1 p + r_1 \text{ and } s = k_2 p + r_2 \text{ by the remainder theorem}$$

$$k \cdot s = (k_1 p + r_1)(k_2 p + r_2)$$

$$= k_1 k_2 p^2 + (k_1 r_2 + k_2 r_1) p + r_1 r_2,$$ where the first two terms are divisible by *p*. So $k \cdot s$ and $r_1 \cdot r_2$ have same remainder when dividing by *p*.

(d) Now, because the remainders of *a*, 2*a*, 3*a*, ... (*p* -1) are congruent to 1, 2, 3, ..., *p*-1, then

$$m=a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \text{ has same remainder as } n=1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1)$$

Here notice $m = (p-1)! \cdot a^{p-1}$ and $n = (p-1)!$.
And (*p*-1)! isn't divisible by *p*, since $(p-1)! = 1 \cdot 2 \cdot ... \cdot (p-1)$ is a product of the numbers non-divisible by *p*. Then we can obtain the desired conclusion that 'a^{p-1} has remainder 1 when dividing by *p*' by dividing both *m* and *n* by (*p*-1)!.