フェルマーの小定理

$a^{p-1}-1 \equiv 0 \pmod{p}$（※）　　ただし、p は素数、a は p と互いに素

p を素数とする。

1、　2、　3、　……　、　p－1　　（1）

これらを b 倍する。ただし b は p と互いに素とする。

b、　2 b、3 b、……　、　（p－1）b　　（2）

（2）の p－1 個の数は、p で割ったときの余りはすべて違います。

背理法で確認しましょう。

mb≡ nb（mod p）とすると、mb－nb≡ 0　つまり　（m－n）b≡ 0
b は p と互いに素なので、m－ n ≡0　m≡ n　m も n も p より小さい自然数なので
m＝ n である。

m≠ n　ならば　　m b ≠ n b（mod p）

（1）（2）の p－1 個の数をすべて掛けると次の関係が成り立つ。

$(p-1)! \equiv (p-1)!\, b^{n-1} \pmod{p}$　　（3）

（p－1）！と p は、互いに素なので　（3）の両辺は（p－1）！で割れるので、

$1 \equiv b^{n-1} \pmod{p}$　　つまり　　（※）が証明できました。

ちょっと実験

1　2　3　4　　（mod　5）

×3倍

3　6　9　12　　3≡3　　6≡1　9≡4　12≡2　（mod　5）

5で割ったときの余りはすべて違う。

4！≡3^4×4！（mod　5）　4！と5は互いに素なので　1≡3^4(mod　5）

問）A＝18^{17}＋17^{18}　は素数か？

素数か？と問われたら、だいたい素数ではない。
※素数の判断は、その値の√A までのすべての素数で割り切れないことを言わないといけない。これ以外の方法はない。

つまり、割り切れる数をみつければよいのだ。

フェルマーの小定理より、17^{18}≡1（mod　19）

18^{17}≡（−1）^{17}　＝−1（mod　19）

つまり、18^{17}＋17^{18}≡−1＋1＝0（mod　19）

Aは19で割り切れるので、素数ではない。