フェルマーの小定理

ａｐ－１―１≡０（modｐ）（※）　　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、　２ｂ、３ｂ、………　、　（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。

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。

対偶をとると

ｍ≠ｎ　ならば　　ｍｂ≠ｎｂ（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）！≡（ｐ－１）！ｂｐ―１（mod 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≡ｂｐ―１（mod 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！≡３４×４！（mod　５）　４！と５は互いに素なので　１≡３４(mod ５)

問）A＝１８１７＋１７１８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、１７１８≡１（mod　１９）

１８１７≡（―１）１７＝―１（mod　１９）

つまり、１８１７＋１７１８≡―１＋１＝０（mod　１９）

Aは１９で割り切れるので、素数ではない。