2022年2月19日

今日の一曲、ないです。

良し

- E - Integer Sequence Fair

[フェルマーの小定理,式変形,modP]

解説を読んで、M^{K^N} をPで割ったあまりを求めるためには、K^NをP-1で割ったあまりrを求めてM^rをpで割ったあまりを求めればいい。ということは理解できたものの、そもそもどうして、

$M^{K^N}\%P \neq M^{(K^N)\%P}\%P$
$M^{K^N mod P}! \equiv M^{K^N}(modP)$ ← 合同式で上の式を書きたかったけど、 ≡ に線入れて合同じゃないっていう記号がなかったので! ≡ で合同じゃないって読んでほ

なんやねん。っていう人(俺)向けに書いた記事です。気持ちとしては、「なんで KのN乗をPで割ったあまりyを求めて、Mのy乗が答えにしちゃだめなの？」っていう記事です。

保身ですが,「**Pが素数じゃなきゃいけないよ、とかそういう話はよく分からないので、厳密なところはコメントなり、記事引用して補足してくれると嬉しいし、読んでる側としては、「何らかの条件(Pが素数じゃなきゃいけない)があるにしても、大体こんな感じなんだな、」っていうのがつかめればいいのかなと思っています。**」

上の式が成り立たないことの説明だけに重点を置くので、もともとの問題を解く(繰り返し二乗法がどうとか)ってところまではやりません

フェルマーの小定理は証明もよく分からないけど、そういうものがあるんだな、って受け入れた前提で話しをします(実際に俺はフェルマーの小定理をよくわかっていないです)

説明は次のように行います。

1. $$M^{K^N}\%P = M^{(K^N)\%P}\%P \cdots (★)$$
   $M^{K^N mod P} \equiv M^{K^N}(modP)$★の式を合同式で書いただけです。同じことを意味しています。多分

   という★の式がが成り立ってくれるためにはどういう条件が成立すればいいのかを考える
2. ★の式が成り立つ条件というものが、が**絶対に**成り立たないことを述べる
3. ★式が絶対に成り立たないので、「なんで KのN乗をPで割ったあまりyを求めて、Mのy乗が答えにしちゃだめなの？」に対する理由付けが出きた

ではまず、さっそくですが、

1. ★の等式が成り立つ条件

   どうやって条件を見つけるのかってことですが、これは1個見つけちゃえばいいので、人(@asakaakasaka)に聞きます。

   その条件とは ,$M^P\%P = 1$,合同式で書くと$M^P \equiv 1(modP)$です。このときに★の式が成り立つことを、数式変形を用いて説明します。

   $$K^N\%P = y\text{と置く}(y \equiv K^N(modP))$$
   $$\text{このとき、}K^N\text{を}P\text{で割ったあまりが}y\text{であるから、商を}t(\text{自然数})\text{として}$$
   $$k^N = tP + y\text{と書くことができる}$$

   上は前提知識というか、説明で使う文字の説明です。

   やや数式がややこしくなるので、合同式で説明したのと、等式で説明したのと2通りを記してあります。好きな方を読んでください。どちらの式も同じことを書いてあるつもりです。

   a. まず、等式で書いたパターン

   $M^P\%P = 1$・・・この式を前提として数式を変形して,★が成り立つことを示す。まず、両辺をt乗する
   $(M^P\%P)^t = 1^t$次に、両辺に$M^y\%P$を掛ける。右辺の1^tは1なので、1にしちゃう
   $(M^P\%P)^t(M^y\%P) = 1\times M^y\%P$　　左辺の$\%P$をくくり出す
   $(M^P)^t(M^y)\%P = M^y\%P$　$(x^a)^b = x^{ab}$みたいな変形をする
   $M^{Pt+y}\%P = M^y\%P$ 文字の定義のところで、$K^N = tP + y$って書けるって話をしたので、
   $M^{K^N}\%P = M^y\%P$
   上記手順により、★の式が成り立つときMの$(K$のN乗$)$乗は、Mの$(K$のN乗をPで割ったあまり乗$)$に等しい

   b. 合同式で書いたパターン

   $M^P \equiv 1(mod\ P)$・・・この式を前提として数式を変形して,★が成り立つことを示す。まず、両辺をt乗する
   $(M^P)^t \equiv 1^t(mod\ P)$次に、両辺に$M^y$を掛ける。右辺の$1^t$は1なので、1にしちゃう
   $(M^P)^t(M^y) \equiv 1\times M^y(mod\ P)$ で、$(x^a)^b = x^{ab}$みたいな変形をする
   $M^{Pt+y} \equiv M^y(mod\ P)$ 文字の定義のところで、$K^N = tP + y$って書けるって話をしたので、
   $M^{K^N} \equiv M^y(mod\ P)$ 右辺のyをyにする
   $M^{K^N} \equiv M^{K^N mod P}(modP)$
   上記手順により、★の式が成り立つときM

長くなりましたが、まとめます。
,$M^P\%P=1$であるとき,合同式で書くと$M^P\equiv 1(modP)$であるときに、

$$M^{K^N}\%P=M^{(K^N)\%P}\%P\cdots(\bigstar)$$
$$M^{K^N}\equiv M^{K^N\%P}(modP)\leftarrow \text{合同式で書いたバージョン}$$

の式が成り立つ。

2. 次に、$M^P\%P=1$であるとき,合同式で書くと$M^P\equiv 1(modP)$が成り立たないことを言います。
    1. フェルマーの小定理に反するので、上の条件が成り立ちません。
    フェルマーの小定理は、次の式です。$M^{(P-1)}\equiv 1(modP)$
    フェルマーの小定理は**なり立ってる**やつなので、これの両辺にMを掛けたものも成り立ちます。合同式のほうだけ書きます。

$$M^{P-1}M\equiv M(modP)$$
$$M^P\equiv M(modP)$$

    この式は、1で示した条件式が成り立たないことを言っています。
    つまり、

> $M^P\%P=1$であるとき,合同式で書くと$M^P\equiv 1(modP)$であるときに、
>
> $$M^{K^N}\%P=M^{(K^N)\%P}\%P\cdots(\bigstar)$$
> $$M^{K^N}\equiv M^{K^N\%P}(modP)\leftarrow \text{合同式で書いたバージョン}$$
>
> の式が成り立つ。

    といいましたが、そもそも、$M^P\%P=1$であるとき,合同式で書くと$M^P\equiv 1(modP)$が成り立たないので、★の式も成り立たない、ということになります。
3. 以上、長くなりましたが、★の式が成り立つ条件を示すー>そのような条件はフェルマーの小定理によりなりたない→よって、★の式は成り立たない、ということが言えました。

結果だけ見ると、

$$M^{K^N}\%P\neq M^{(K^N)\%P}\%P$$
$$M^{K^N mod P}!\equiv M^{K^N}(modP)$$

であることを示したことになっていると思います。お疲れさまでした。

謝辞

https://twitter.com/asakaakasaka?s=20&t=EggWpSoiNyqxn5TC3dDYww

まじ感謝