2017 年度 中間試験の問題の一部の解答例

10A. n は自然数で, $p=2^n+1$ は素数であるとせよ.
(その様な p は Fermat 素数 と呼ばれる.)
(1) $p>5$ ならば 2 は法 p の原始根ではないことを示せ.
(2) $p>3$ ならば 3 は法 p の原始根であることを証明せよ.

(Hint : 法 p で -1 が平方元であることを示せ. もし, 3 が原始根でないのなら平方元であることを示せ. それゆえ, $-3\equiv a^2 \mod p$ なる a が存在する. このとき $2u\equiv -1+a \mod p$ で定まる u は位数が 3 であることを示せ. これと Fermat の小定理から $3|p-1$ を示し, 矛盾を導け.)

解. 以下, ときに $\bmod p$ を指示する $\bar{}$ を省いて書く.
(1) $2^n\equiv -1 \mod p$ より $2^{2n}\equiv 1 \mod p$ となり, Fermat の小定理と合はせると, $2n|p-1$ つまり $2n|2^n$ なので, n は 2 の冪である. それゆえ, $\operatorname{ord} 2 = 2n$ である (**10B** の解答を参照せよ). もし 2 が原始根であれば $2n = p-1 = 2^n$ となるが, これは $n>2$ であれば $2n<2^n$ となるので, 成り立たない.
(2) $p\equiv 1 \mod 4$ なので -1 は法 p の平方剰余である. 3 が原始根でないとすると $3^{2^{n-1}} = 3^{(p-1)/2}\equiv 1 \bmod p$ である. 法 p の原始根を g として $3=g^t$ とすると $g^{t2^{n-1}} = 3^{2^{n-1}} = 1$ なので $p-1\,|\,t2^{n-1}$ 即ち $2^n|t2^{n-1}$. つまり $2|t$ がわかり, 3 は平方元である. よつて $-3=-1\cdot 3$ も平方元である. $-3\equiv a^2 \mod p$ とおける. ここで $2u\equiv -1+a \mod p$ となる u を取る ($\gcd(2,p)=1$ だからその様な u が存在する). この式を立方すれば

$$\begin{aligned} 8u^3 &\equiv -1+3a-3a^2+a^3 \mod p \\ &\equiv -1+3a-3(-3)+(-3)a \mod p \\ &= 8 \\ \therefore u^3 &\equiv 1 \mod p \end{aligned}$$

を得るが, 容易に $u\not\equiv 1 \bmod p$ がわかり $\operatorname{ord} u = 3$ である (もし $u\equiv 1 \bmod p$ なら $a\equiv 3 \bmod p$ なので $-3\equiv 3^2 \bmod p$ となり $p>3$ に反する). しかるに, Fermat の小定理によれば $3\,|\,p-1$ 即ち $3\,|\,2^n$ でなければならないから, 矛盾である.

10B. p は奇素数であつて, $a^{2^n}+1$ の約数であるとせよ. このとき $p\equiv 1 \mod 2^{n+1}$ であることを示せ.
(Hint : $(a \mod p)$ の $(\mathbb{Z}/p\mathbb{Z})^\times$ における位数を求めよ.)

解. 仮定より

$$a^{2^n}\equiv -1 \mod p. \tag{a}$$

これより

$$a^{2^{n+1}}\equiv 1 \mod p. \tag{b}$$

この 2 式から $\operatorname{ord} a = 2^{n+1}$ がわかる. 実際, (b) から $\operatorname{ord} a$ は 2^{n+1} の約数であるが, (a) から $\operatorname{ord} a$ は 2^k $(0\le k\le 2^n)$ ではないからである. 一方, 仮定から $p\nmid a$ なので Fermat の小定理から

$$a^{p-1}\equiv 1 \mod p.$$

即ち $\operatorname{ord} a$ は $p-1$ の約数である. 以上から

$$2^{n+1}|p-1$$

がわかり

$$\begin{aligned} p-1 &\equiv 0 \mod 2^{n+1} \\ \therefore\ p &\equiv 1 \mod 2^{n+1}. \end{aligned}$$