A. ŁAPAREWICZ.

CECHA PODZIELNOŚCI LUCASA.

Jakkolwiek swą cechę podzielności, dogodną szczególniej względem liczb wzoru $2^n \pm 1$, ogłosił był Lucas[1] już przed 30 tu niemal laty, ze względu jednak na to, że nigdzie dotąd u nas nie została ona uwzględniona, a stosunek jej do liczb 2^n-1, związanych z nazwiskiem naszego uczonego Jana Brożka, którego prace na tem polu przyczyniły się niewątpliwie do wykrycia przez Fermata twierdzenia ogólnego, czyni ją dla nas podwójnie ciekawą, uważam za właściwe temat ten obecnie poruszyć.

Weźmy dwie funkcye liczebne:

$$(1) \qquad U_n = \frac{a^n - b^n}{a - b}, \quad V_n = a^n + b^n,$$

gdzie a i b są pierwiastkami równania kwadratowego:

$$x^2 = Px - Q,$$

o spółczynnikach P i Q całkowitych i niespółdzielnych.

Ponieważ w ten sposób $a+b=P$, $ab=Q$, przeto: $\sqrt{P^2-4Q}=a-b$, którą to różnicę oznaczamy przez δ; własności powyższego równania

[1]) Lucas „Théorie des fonctions numériques simplement périodiques“ (Amer. Journ., t. I).

w znacznej mierze zależą od kwadratu tej różnicy, zwanego wyróżnikiem równania i oznaczanego przez Δ, tak, iż:

$$\Delta = P^2 - 4Q. \tag{2}$$

Z określenia wielkości U i V wynika bezpośrednio:

$$V_n + \delta U_n = 2a^n, \quad V_n - \delta U_n = 2b^n, \tag{3}$$

tak, iż kładąc raz $n = \alpha$, następnie $n = \beta$ i mnożąc otrzymane wypadki stronami, kładąc wreszcie $n = \alpha + \beta$, znajdziemy:

$$(V_\alpha \pm \delta U_\alpha)(V_\beta \pm \delta U_\beta) = 2(V_{\alpha+\beta} \pm \delta V_{\alpha+\beta}), \tag{4}$$

z zachowaniem odpowiedniości znaków.

Z (4) w razie $\beta = \alpha$ wynika:

$$V_{2\alpha} \pm \delta U_{2\alpha} = \tfrac{1}{2}(V_\alpha^2 \pm 2\delta U_\alpha V_\alpha + \Delta V_\alpha^2)$$

tak iż:

$$U_{2\alpha} = U_\alpha V_\alpha, \quad 2V_{2\alpha} = V_\alpha^2 + \Delta U_\alpha^2. \tag{5}$$

Że zaś mnożąc (3) stronami, mamy:

$$V_\alpha^2 - \Delta U_\alpha^2 = 4Q^\alpha, \tag{6}$$

przeto drugi ze wzorów (5) można przedstawić w postaci:

$$V_{2\alpha} = V^2{}_\alpha - 2Q^\alpha. \tag{5a}$$

Z (4) wreszcie, po wykonaniu wskazanego mnożenia, dodając i odejmując otrzymane wzory stronami, znajdziemy:

$$2V_{\alpha+\beta} = V_\alpha V_\beta + \Delta U_\alpha U_\beta; \quad 2U_{\alpha+\beta} = U_\alpha V_\beta + V_\alpha U_\beta. \tag{7}$$

Wzór (6) wskazuje, że wspólny dzielnik liczb U_n i V_n jest również dzielnikiem liczby Q; z rozwinięcia zaś $(a+b)^n = P^n$, po połączeniu wyrazów równooddalonych od jego początku i końca, wynika $V_n \equiv P^n \pmod{Q}$, co dowodzi, że wspólny dzielnik liczb V_n i Q jest dzielnikiem liczby P. Zatem wspólny dzielnik liczb U_n i V_n jest zarazem i wspólnym dzielnikiem liczb P i Q; że zaś te ostatnie, według założenia są niespółdzielne, przeto

I. Liczby U_n i V_n są niespółdzielne.

Ponieważ drugi ze wzorów (7) wskazuje, że jeżeli $U_{\alpha+\beta}$ i U_β mają wspólny dzielnik, przez tenże będzie podzielny i iloczyn $U_\alpha V_\beta$, przeto na zasadzie I wnosimy, że ten wspólny dzielnik będzie dzielnikiem liczby U_α. Stąd wynika, że jeżeli U_m i U_n, gdzie $m > n$, mają wspólny dzielnik, będzie przez niego podzielną i U_{m-n}; następnie, wspólny dzielnik liczby U_n i U_{m-n} będzie także dzielnikiem liczby U_{m-2n} i t. d.: wnosząc w końcu, że wspólny dzielnik liczby U_m i U_n będzie wspólnym dzielnikiem liczb U_{n_1} i U_m, gdzie $n_1 = m - kn$. Podobnież, wspólny dzielnik liczb U_n i U_{n_1} będzie wspólnym dzielnikiem liczb U_{n_1} i U_{n_2}, gdzie $n_2 = n - k_1 n_1 < n_1$ i t. d. Zatem ostatecznie:

II. Wspólny dzielnik liczby U_m i U_n jest zarazem dzielnikiem liczby U_l gdzie l jest największym wspólnym dzielnikiemliczby m i n

Zważywszy, że $2a = P + \delta$, $2b = P - \delta$ mamy:

$$2^n a^n = P^n + \frac{n}{1} P^{n-1}\delta + \frac{n(n-1)}{2!} P^{n-2}\delta^2 + \ldots\ldots + \frac{n}{1} P\delta^{n-1} + \delta^n,$$

$$2^n b^n = P^n - \frac{n}{1} P^{n-1}\delta + \frac{n(n-1)}{2!} P^{n-2}\delta^2 - \ldots + (-1)^{n-1}\frac{n}{1} P\delta^{n-1} + (-1)^n \delta^n;$$

odejmując stronami i dzieląc przez δ, znajdziemy:

$$(8) \qquad \begin{aligned} 2^{n-1} U_n = {} & \frac{n}{1} P^{n-1} + \frac{n(n-1)(n-2)}{3!} P^{n-3}\Delta + \\ & + \frac{n(n-1)(n-2)(n-3)(n-4)}{5!} P^{n-5}\Delta^2 + \ldots\ldots \end{aligned}$$

przyczem ostatnim wyrazem będzie $\frac{n}{1} P\Delta^{\frac{n-2}{2}}$ lub $\Delta^{\frac{n-1}{2}}$, stosownie do tego, czy n jest liczbą parzystą czy nieparzystą.

Kładąc teraz $n = p \pm 1$, gdzie p jest liczbą bezwzględnie pierwszą nieparzystą, mamy stąd:

$$(9) \qquad \begin{cases} 2^p U_{p+1} = \frac{p+1}{1} P^p + \frac{(p+1)p(p-1)}{3!}\Delta P^{p-2} + \ldots\ldots + \frac{p+1}{1}\Delta^{\frac{p-1}{2}} P \\ 2^{p-2} U_{p-1} = \frac{p-1}{1} P^{p-2} + \frac{(p-1)(p-2)(p-3)}{3!}\Delta P^{p-4} + \ldots\ldots + \frac{p-1}{1}\Delta^{\frac{p-3}{2}} P. \end{cases}$$

Pierwsza z tych równości, w której wszystkie wyrazy prawej strony, z wyjątkiem dwu skrajnych, są podzielne przez p, prowadzi do kongruencyi $2^p U_{p+1} \equiv P(P^{p-1} + \Delta^{\frac{p-1}{2}}) \pmod p$. Co zaś do drugiej, to zważając, że wszystkie spółczynniki, których wzorem ogólnym jest $\frac{(p-1)\ldots(p-k)}{k!} = A_k$, są liczbami całkowitemi, a $(p-1)\ldots(p-k) = pf_{k-1}(p) + (-1)^k k!$ gdzie $f_{k-1}(p)$ jest funkcyą całkowitą $k-1$ stopnia względem p, mamy $A_k = p\frac{f_{k-1}(p)}{k!} + (-1)^k$, tak iż $\frac{f_{k-1}(p)}{k!}$ jest również liczbą całkowitą i $A_k \equiv (-1)^k \pmod p$, zatem według mod p jest:

$$2^{p-2} U_{p-1} \equiv -P^{p-2} - \Delta P^{p-4} - \ldots - \Delta^{\frac{p-3}{2}} P \equiv -P\frac{P^{p-1} - \Delta^{\frac{p-1}{2}}}{P^2 - \Delta}.$$

Zamiast więc równości (9), mamy do rozważania kongruencye:

$$2^p U_{p+1} \equiv P(P^{p-1} + \Delta^{\frac{p-1}{2}}), \quad 2^{p-2} U_{p-1} \equiv -P\frac{P^{p-1} - \Delta^{\frac{p-1}{2}}}{P^2 - \Delta} \pmod p.$$

Ponieważ P zawsze możemy obrać liczbą niespółdzielną p, tak iż $P^{p-1} \equiv 1 \pmod p$, przeto, stosownie do tego, czy:

$$\Delta^{\frac{p-1}{2}} \equiv -1 \quad \text{czy} \quad +1 \pmod p$$

otrzymamy ostatecznie:

$$U_{p+1} \equiv 0 \quad \text{lub} \quad U_{p-1} \equiv 0 \pmod p, \text{ t. j.}$$

III. W szeregu liczb U o wskaźnikach kolejnych zawsze znajdzie się wyraz U_{p-1} lub U_{p+1} podzielny przez liczbę pierwszą p; przyczem wyrazem takim będzie U_{p-1}, jeżeli wyróżnik równania, z którego pierwiastków funkcye te tworzymy, będzie resztą, a U_{p+1} jeżeli niereszta liczby pierwszej p.

Z teoryi reszt potęgowych wynika, że jeżeli p jest liczbą pierwszą, a c niespółdzielną z p, to kongruencya $c^x \equiv 1 \pmod p$, zawsze mająca miejsce, według Fermata, dla $x = p-1$, może się sprawdzać i dla $x < p-1$. Zatem kongruencya $U_x \equiv 0 \pmod p$, gdzie p jest liczbą pierwszą, prócz $x = p \pm 1$, może mieć miejsce i dla $x = m < p \pm 1$. Lecz z podzielności liczb $U_{p\mp1}$ i U_m przez p, według II, wynika podziel-

ność przez p i liczby U_n, gdzie n jest największym wspólnym dzieln. $p \pm 1$ i m. Stąd wnosimy, że $\frac{p \mp 1}{n} = k$ jest liczbą całkowitą, tak iż dzielnik liczby U_n winien być wzoru $p = nk \pm 1$, gdzie 1 należy wziąć z $+1$ lub -1, stosownie do tego, czy Δ jest resztą czy niereszta liczby p, co wyrazimy pisząc $p = nk + \left(\frac{\Delta}{p}\right)$. Że zaś $U_{2n} = U_n V_n$, a U_n i V_n są niespółdzielne, przeto dzielnik liczb V_n winien być wzoru $p = 2nk + \left(\frac{\Delta}{p}\right)$.

Że zaś nadto, według (6) $V_n^2 - 4Q \equiv 0 \pmod{U_n}$ lub $\Delta^2 U_n^2 + 4Q^n \Delta \equiv 0 \pmod{V_n}$, przeto dzielniki liczby U_n dla nieparzystych wskaźników są dzielnikami formy $x^2 - Qy^2$, dzielniki zaś liczby V_n są dzielnikami formy $x^2 + \Delta y^2$ lub $x^2 + \Delta Q y^2$, stosownie do tego, czy n jest liczbą parzystą czy nie. Zatem:

IV. Liczby U_n są podzielne przez liczby pierwsze wzoru $kn + \left(\frac{\Delta}{p}\right)$, które jednocześnie są dzielnikami formy $x^2 - Qy^2$, liczby zaś V_n—przez liczby pierwsze $p = 2kn + \left(\frac{\Delta}{p}\right)$, które jednocześnie są dzielnikami formy $x^2 + \Delta y^2$, gdy n jest liczbą parzystą, lub $x^2 + \Delta Q y^2$, gdy nieparzystą.

Zauważmy, że, jak to wynika ze sposobu dowodzenia tw. III kongruencya $U_{p \mp 1} \equiv 0 \pmod{p}$ jest niemożliwą bez założenia, że p jest liczbą pierwszą. Co zaś do kongruencyi $U_n \equiv 0 \pmod{p}$ gdy $n < p \pm 1$, a p jest liczbą złożoną, to można okazać, że w niektórych przypadkach szczególnych dałaby się ona urzeczywistnić. Np. jeżeli przypuścimy że $p = lm$, gdzie l i m są liczbami pierwszemi, tak iż według III $U_{l \mp 1} \equiv 0 \pmod{l}$, $U_{m \mp 1} \equiv 0 \pmod{p}$ czyli $m U_{l \mp 1} \equiv 0$ $l U_{m \mp 1} \equiv 0 \pmod{p}$, to zakładając $m \equiv V_{m \mp 1}$, $l \equiv V_{l \mp 1} \pmod{p}$, na zasadzie (7) otrzymalibyśmy $U_n \equiv 0 \pmod{p}$, gdzie $n = (l \mp 1) + (m \mp 1) < p \mp 1$ [1].

---

[1]) Stąd wynika, że błędnem jest twierdzenie odwrotne względem twierdzenia III, które Lucas w następny wyraził sposób: Jeżeli kongruencya $U_n \equiv 0 \pmod{p}$ ma miejsce dopiero dla $n = p \mp 1$, a dla żadnej wartości na $n < p \mp 1$ nie daje się urzeczywistnić, wówczas liczba p jest bezwzględnie pierwszą. Przez dziwne jakieś niedopatrzenie Lucas w warunkach obecnego twier-

Z twierdzenia III wynika bardzo piękna cecha podzielności liczb wzoru $2^n \pm 1$. Jakoż, jeżeli położymy na Δ wartość taką, aby $\left(\frac{\Delta}{2^n \pm 1}\right) = \pm 1$ (z zachowaniem odpowiedniości znaków), wtedy warunek konieczny, by liczba $2^n \pm 1$ była pierwszą, wyrazi się w postaci kongruencyi $U_{2^n} \equiv 0 \pmod{2^n \pm 1}$. Lecz na zasadzie (5) i z uwzględnienieniem, że $U_{2^0} = 1$, warunek ten prowadzi do tego, aby w szeregu

$$V_{2^0},\ V_{2^1},\ V_{2^2},\ \ldots\ldots\ V_{2^{n-1}}, \tag{10}$$

jeden z wyrazów był podzielny przez $2^n \pm 1$. Ten ostatni warunek nie jest jednak w tym celu dostateczny, ponieważ, jak widzieliśmy, kongruencya $U_m \equiv 0 \pmod{p}$ może niekiedy się sprawdzać i w razie gdy p jest liczbą złożoną, tak iż podzielność przez $2^n \pm 1$ któregokolwiek wyrazu w szeregu (10) nie dowodzi jeszcze, aby $2^n \pm 1$ było liczbą pierwszą.

Wiedząc to, przypuśćmy, że $V_{2^\alpha} \equiv 0 \pmod{2^n \pm 1}$ i że $2^n \pm 1$ jest liczbą złożoną; w takim razie czynniki liczby $2^n \pm 1$ winne być czynnikami liczby V_{2^α}, które, według twierdz. IV, mają być wzoru $2^{\alpha+1}k + \left(\frac{\Delta}{2^n \pm 1}\right)$, że zaś przynajmniej jeden z nich jest $< \sqrt{2^n \pm 1}$, przeto jeżeli przy najmniejszej wartości na k, t. j. 1, wyrażeniu $2^{\alpha+1}k + \left(\frac{\Delta}{2^n \pm 1}\right)$ nadamy największą możliwą wartość, t. j. $\sqrt{2^n \pm 1}$, to równość $\left\{2^{\alpha+1} + \left(\frac{\Delta}{2^n \pm 1}\right)\right\}^2 = 2^n \pm 1$ przyczyni się do określenia największej wartości na α, dla której podzielność liczby V_{2^α} przez $2^n \pm 1$ pozwala na przypuszczenie, że $2^n \pm 1$ może być liczbą złożoną. Zważając zaś, że w przytoczonej równości drugie wyrazy obu stron nikną w porównaniu z pierwszemi, znajdziemy stąd $2(\alpha+1) = n$, tak iż $\alpha < \frac{n-1}{2}$. Zatem:

---

dzenia zaprzeczył temu, co sam przyjął za pewnik, dowodząc twierdzenia IV, dowód zaś oparł widocznie na własności $U_\alpha U_\beta U_\gamma \ldots = U_{\alpha+\beta+\gamma+\ldots}$, której, jak wskazuje wzór (7), funkcya U nie posiada. Na szczęście twierdzenie to na dalsze wnioski z twierdzenia III nie wpływa.

V. Jeżeli w szeregu (10) pierwszym wyrazem podzielnym przez $2^n \pm 1$, jest $V_{2\alpha}$, to, o ile $\alpha \geqq \frac{n-1}{2}$, liczba $2^n \pm 1$ jest liczbą pierwszą, w razie zaś $\alpha < \frac{n-1}{2}$ liczba $2^n \pm 1$ może być liczbą złożoną, podzielną przez $2^{\alpha+1} + \left(\frac{\Delta}{2^n \pm 1}\right)$ (lecz również może być i liczbą pierwszą); jeżeli wreszcie żaden z n wyrazów szeregu (10) nie jest przez $2^n \pm 1$ podzielnym, wtedy liczba $2^n \pm 1$ jest liczbą złożoną, lecz czynników jej tą drogą nie wykryjemy [1].

[1]) Wrazie $\alpha < \frac{n-1}{2}$, zdaniem Lucasa, liczba $2^n \pm 1$, będąc dzielnikiem liczby $V_{2\alpha}$) stanowczo jest liczbą złożoną; z dowodzenia jednak powyższego pewność ta bynajmniej nie wypływa. Co większa, z tak kategorycznego twierdzenia możnaby wyprowadzić wniosek, że szereg $2^{2^m}+1$, w którym Fermat upatrywał jedynie liczby pierwsze, począwszy od pewnej wartości na m zawierałby tylko liczby złożone, tak iż sławne twierdzenie Eisensteina, że szereg $2+1$, 2^2+1, $2^{2^2}+1$, $2^{2^{2^2}}+1$..... przedstawia same liczby pierwsze, byłoby ostatecznie rozstrzygnięte w sensie odmownym. Jakoż przy wyborze liczb V, potrzebnych do określenia składu liczby 2^n+1, winno być $\left(\frac{\Delta}{2^n+1}\right) = +1$; warunkowi temu odpowiada równanie o pierwiastkach wymiernych, ponieważ Δ w takim razie jest liczbą kwadratową, z równań zaś takich najprostszem jest równanie, dla którego $a=2$, $b=1$, szereg zaś (10) staje się szeregiem $2^{2^0}+1$, $2^{2^1}+1$,....$2^{2^{n-1}}+1$. Przy takim wyborze szeregu V, pierwsza część twierdzenia Lucasa sprowadza się do tego, że jeżeli w szeregu $2^{2^0}+1$, $2^{2^1}+1$, $2^{2^2}+1$,... ..$2^{2^n}+1$ wyraz identyczny z 2^n+1, co jest możliwem tylko wrazie, gdy n jest potęgą liczby 2, przypada w pierwszej tegoż połowie, wtedy 2^n+1 jest liczbą złożoną. Lecz jeżeli kładziemy na n kolejne potęgi liczby 2, tak iż liczba wyrazów szeregu stopniowo się podwaja, wtedy wyraz identyczny z 2^n+1 będzie się przesuwał o jedno miejsce ku prawej ręce, tak iż, jakkolwiek w razie niższych potęg wyraz taki będzie się znajdował w drugiej połowie szeregu, stopniowo jednak przejdzie do pierwszej, a raz tam przeszedłszy, już dla wszystkich wyższych potęg liczby 2 w niej pozostanie. Stąd wynika, że liczby $2^{2^m}+1$, pierwsze dla niższych wartości m, dla wszystkich wyższych m winny już być stale liczbami złożonemi. Lecz kładąc po kolei $m=1,2,3,...$, znajdujemy w ten sposób, że już $2^{2^4}+1$ musiałaby być złożoną, gdy wiemy, że dopiero $2^{2^5}+1$ jest podzielną przez 641, a $2^{2^4}+1$ w rzeczy samej jest liczbą pierwszą. Stąd wnosimy, że w warunkach, wyszczególnionych w pierwszej części twierdzenia Lucasa, złożoność rozważanej liczby jest jedynie możliwą, lecz bynajmniej nie udowodnioną w sposób stanowczy.

Pozostaje do omówienia kwestya wyboru $\Delta = P^2 - 4Q$. Ponieważ w ten sposób Δ nie zależy od znaku P, z określenia zaś V wynika $V_{2^0} = P$, na dalsze zaś V znak P, według (5a) nie wpływa, przeto można poprzestać na $P > 0$. Co zaś do Q, to wzór (5a) wskazuje, że najdogodniej przyjąć $Q = \pm 1$; zważając bowiem, że w danym razie wszystkie wskaźniki V, z wyjątkiem pierwszego, są parzyste, w razie $Q = +1$ dla wszystkich, a w razie $Q = -1$ poczynając od trzeciego, będziemy mieli: $V_{2a} = V_a^2 - 2$, t. j. każdy z nich będziemy otrzymywali kolejno jako zmniejszony o 2 kwadrat poprzedzającego. (W razie $Q = -1$ drugi wyraz będzie kwadratem pierwszego powiększonym o 2). Kładąc więc $Q = \pm 1$, a za P po kolei 1,2,3,... znajdziemy szereg wartości na Δ które przyjmujemy lub odrzucamy stosownie do tego, czy odpowiadają warunkowi $\left(\frac{\Delta}{2^n \pm 1}\right) = \pm 1$ czy nie.

W razie $P_1 = 1$, stosownie do tego, czy $Q = +1$ czy -1, mamy $\Delta = -3$ lub $+5$. Zważając zaś, że $\left(\frac{-3}{2^n \pm 1}\right) = \left(\frac{2^n \pm 1}{3}\right)$, a $2 \equiv -1 \pmod 3$ tak iż $2^n \pm 1 \equiv (-1)^n \pm 1 \pmod 3$, wnosimy, że w razie n parzystego $\left(\frac{2^n - 1}{3}\right) = +1$, w pozostałych zaś $2^n \pm 1 \equiv 0 \pmod 3$, tak iż -3 w żadnym razie na Δ się nie nadaje. Co zaś do $\Delta = 5$, to zważając, że $\left(\frac{5}{2^n \pm 1}\right) = \left(\frac{2^n \pm 1}{5}\right)$ a $2^2 \equiv -1 \pmod 5$, tak iż $2^{2n+1} \pm 1 \equiv 2(-1)^n \pm 1 \pmod 5$, skąd w razie n parzystego $2^{2n+1} + 1 \equiv 3$, $2^{2n+1} - 1 \equiv 1$, nieparzystego $2^{2n+1} + 1 \equiv 4$, $2^{2n+1} - 1 \equiv 2 \pmod 5$, wnosimy, że $\Delta = 5$ służy do badania liczb $2^{2n+1} \pm 1$ w razie, gdy n jest liczbą nieparzystą, czyli prościej liczb $2^{4m+3} \pm 1$, że zaś $2^{4m+3} + 1$ ak wiemy, zawsze jest złożoną, przeto do $\Delta = 5$ uciekamy się przy badaniu składu liczb $2^{4m+2} - 1$; do tegoż samego wniosku dojdziemy prędzej, wychodząc z kongruencyi $2^4 = 1 \pmod 5$. W razie $P = 2$ mamy $\Delta = 0$ lub $\Delta = 8$; w pierwszym razie, na zasadzie wzoru (5) mamy $2V_{2a} = V_a^2$, a że $V_1 = 2$, przeto wszystkie V są równe 2, tak iż w tym razie z góry jest przesądzona niepodzielność każdej liczby V przez $2^n \pm 1$; co zaś do $\Delta = 8$, to zważając, że $\left(\frac{\Delta}{2^n \pm 1}\right) = \pm 1$, a $\left(\frac{8}{2^n \pm 1}\right) = \left(\frac{2}{2^n \pm 1}\right)$, wnosimy, że winno być: $2^n + 1 \equiv 1$ lub 7, $2^n - 1 \equiv 3, 5$

(mod 8); lecz kongruencye $2^n+1\equiv 7$, $2^n-1\equiv 5$, prowadząc do $2^n\equiv 6 \pmod 8$, niepodobne są osiągnięcia, $2^n-1\equiv 3$ sprawdza się jedynie dla $n=2$, wreszcie $2^n+1\equiv 1 \pmod 8$ jest możliwą dla każdej wartości na $n\geqq 3$, tak iż $\Delta=8$ może służyć jedynie do badania 2^n+1, począwszy od $n=3$. Wrazie $P=3$, prócz zbadanego poprzednio $\Delta=5$, otrzymujemy $\Delta=13$; zważając, że stosownie do tego, czy $n\equiv 0,1,2,...11 \pmod{12}$, mamy $2^n\equiv 1,2,4,8,3,6,12,11,9,5,10,7 \pmod{13}$, oraz że resztami 13 są 1, 3, 4, 9, 10 i 12 a $\left(\frac{13}{2^n\pm 1}\right)=\left(\frac{2^n\pm 1}{13}\right)$, wnosimy, że $\Delta=13$ nadaje się do badania składu liczb 2^n-1 w razie $n\equiv 3,4,5,6,8,11 \pmod{12}$, a liczb 2^n+1 w razie $n\equiv 1,3,5,7,8 \pmod{12}$ W ogóle, jeżeli za wyróżnik przyjmiemy liczbę pierwszą nieco większą warunki jego stosowalności otrzymujemy w formie niełatwej do spamiętania, stąd przenosimy zwykle wyróżniki, złożone z liczb najprostszych. W razie $P=4$, mamy $\Delta=12$ lub $\Delta=20$. Co do pierwszego, to zważając, że $\left(\frac{12}{p}\right)=\left(\frac{3}{p}\right)$ a $\left(\frac{3}{2^n\pm 1}\right)=\pm\left(\frac{2^n\pm 1}{3}\right)$ i rozumując jak powyżej, w razie $\Delta=-3$ wnosimy, że $\Delta=12$ nadaje się do badania liczb 2^n-1 dla nieparzystych n; że zaś dla $2^{4m+3}-1$ przyjęliśmy już $\Delta=5$, przeto do $\Delta=12$ uciekać się będziemy w razie $2^{4m+1}-1$. Co zaś do $\Delta=20$, to ponieważ $\left(\frac{20}{p}\right)=\left(\frac{5}{p}\right)$, wszystko, cośmy znaleźli dla $\Delta=5$, stosuje się i obecnie. Następnie $P=5$ prowadzi do mało dogodnych wyróżników 21 i 29, wreszcie dla $P=6$ otrzymujemy 32 i 40, które łatwo sprowadzić do rozpatrzonych poprzednio 8 i 5. Na tem badanie poszczególnych wyróżników możemy zakończyć, przychodząc do następujących wyników, obejmujących wszelkie możliwe przypadki:

I. Do badania liczb $2^{4m+3}-1$ najdogodniejszym jest wyróżnik $\Delta=5$ równań $x^2=x+1$ lub $x^2=3x-1$; rozważając pierwsze równanie, otrzymujemy kolejno: $V_{2^0}=1$, $V_{2^1}=3$, $V_{2^2}=7$..., z drugiego zaś $V_{2^0}=3$, $V_{2^1}=7$..., tak iż począwszy od wyrazu $=3$, oba szeregi będą zgodne. Można również w tym razie uciekać się do $\Delta=20$ lub 40, z których pierwszy jest wyróżnikiem równania $x^2=4x+1$, wytwarzającego szereg 4, 18, 322... drugi zaś $x^2=6x+1$, prowadzącego do szeregu 6, 38, 1242.....

II. Do badania liczb 2^n-1, gdzie n jest jakąkolwiek liczbą nieparzystą (w szczególnym zaś wypadku do badania liczb $2^{4m+1}-1$),

uciekamy się do $\Delta=12$, wyróżnika $x^2=4x-1$, z którego pierwiastków tworzymy szereg V: 4, 14,.....

III. Do badania liczb 2^n+1, gdzie n jest jakąkolwiek liczbą $\geqq 3$, najdogodniej brać $\Delta=8$ lub $\Delta=32$; odpowiednie im równania $x^2=2x+1$ i $x^2=6x-1$ prowadzą do szeregów 2, 6, 34... lub 6, 34..., które, jak widzimy, począwszy od wyrazu $=6$, są zgodne.

Oczywista, że zamiast powyższych liczb, można w rachunek wprowadzać ich bezwzględnie najmniejsze reszty (mod. $2^n \mp 1$).

Do uproszczenia wykonywanych tu rachunków wielce się przyczynia układ dwójkowy, zwłaszcza że unikamy w takim razie dzielenia poszczególnych V przez $2^n \mp 1$: skoro bowiem $2^n \equiv \pm 1$ (mod. $2^n \mp 1$), przeto $2^{n+m} \equiv \pm 2^m$ (mod. $2^n \mp 1$); jeżeli przeto przytrafi się w rachunku jednostka rzędu wyższego nad n, zastępujemy ją zaraz jednostką, której rząd jest nadmiarem tamtego ponad n, przyczem w razie liczb 2^n+1 należy pamiętać, że otrzymana w ten sposób jednostka jest ujemną.

Postępując podanym sposobem, Pierwuszin dowiódł, że liczba:

$$2^{61}-1 = 2\,305\,843\,009\,213\,693\,951$$

jest liczbą pierwszą [1], co najwymowniej przekonywa o skuteczności sposobu Lucasa, ponieważ na wypróbowanie podzielności tej liczby przez wszystkie liczby pierwsze, $\equiv 1$ (mod. 61) i $\equiv \pm 1$ (mod. 8), aż do liczb $\sqrt{2^{61}-1}$ włącznie, należałoby poświęcić 15 lat usilnej pracy, czyli że wynik powyższy przy użyciu sposobu dotychczasowego był nie do osiągnięcia.

Przypisek. Wielce zbliżoną do powyższej cechy podzielności liczb $2^n \pm 1$ można bezpośrednio wyprowadzić z twierdzenia Fermata, jak to postaramy się wykazać w następnym artykule, który zawierać będzie i bliższe wyjaśnienie wyżej wspomnianych rachunków w układzie dwójkowym.

---

[1]) Zapiski Imp. Ak. Nauk. t. 48. Bulletin de l'Ac. de SPB. t. XXXI. str. 532