jejíž pomocí lze pak v takovém případě rozhodnouti, zda se jedná o prvočíslo či ne. (Některé takové případy najdete v knize K. Rychlík: Úvod do elementární teorie číselné, Praha 1931, kde také najdete i jinak provedený důkaz zobecněné věty 1. a věty 2.) A jsou také i jiné postupy, než jaký představuje věta 3.

Konečně uvedu vám alespoň jedny tabulky této věci se týkající, velmi obsáhlé. Jsou to: Lehmer: Factor table for the first ten millions, Washington, 1909. V nich je ke každému číslu nedělitelnému 2, 3, 5, 7 od 0 do 10 017 000 uveden nejmenší kladný celý dělitel.

Důkaz velké Fermatovy poučky pro exponent 4.

Dr. *Jos. Matoušek*, Jindř. Hradec.

Věta Fermatova pro exponent 4 praví:

Číselná rovnice

$$X^4 + Y^4 = Z^4 \text{ při } X, Y, Z > 0^{1})$$

jest nemožnou.

Elementární naukou o číslech provedli důkaz o tom již Euler a Dr. Edmund Landau. Oba tito vědci předpokládají při svých důkazech znalost řešení rovnice $X_1^2 + Y_1^2 = Z_1^2$ celými čísly, na němž své další vývody zakládají. Hodlám zde ukázati, že důkaz dá se provésti přímým způsobem, t. j. bez znalosti řešení rovnice $X_1^2 + Y_1^2 = Z_1^2$.

Zkrátíme-li číselnou rovnici $X^4 + Y^4 = Z^4$ největším společným dělitelem, obdržíme novou $x^4 + y^4 = z^4$, v níž veličiny x, y a z jsou mezi sebou relativně nesoudělné. Dvě z nich musí tedy býti lichými a třetí jest sudou, poněvadž ani součet ani rozdíl dvou lichých čísel nemůže býti lichým. Jedna z veličin x a y jest tudíž určitě lichou. Budiž x liché; pak se snadno přesvědčíme, že y musí býti sudé [součet dvou lichých bikvadrátů — číselně $8h + 1 + 8k + 1 = 2(4l + 1)$ — nemůže býti bikvadrátem.[2]]

Seznali jsme tedy, že v naší rovnici $x^4 + y^4 = z^4$ veličiny x, y a z jsou mezi sebou relativně nesoudělné, y jest číslo sudé, x a z čísla lichá.

Rovnici tuto ve tvaru $z^4 - y^4 = x^4$ rozložíme ve faktory

$$(z^2 + y^2)(z^2 - y^2) = x^4.$$

---

[1]) V celém článku značí nám latinská písmena — velká či malá, s indexem či bez něho — vždy jen čísla celistvá, positivní a konečná.

[2]) Že lichý bikvadrát lze psáti ve tvaru $8h + 1$, je patrno z rovnice

$$(2k + 1)^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1 = 8h + 1.$$

Z uvedených právě vlastností těchto veličin plyne:

$$z^2 + y^2 = f = x_1^4 = u^2$$
$$z^2 - y^2 = g = x_2^4 = v^2$$
$$x^4 = x_1^4 x_2^4 = u^2 v^2$$

Rovnice $f = x_1^4$, $g = x_2^4$ můžeme psáti, poněvadž f a g (obě liché) nemohou míti žádného společného dělitele; event. společný dělitel musil by se jinak také objeviti při číslech z a y. Pro zjednodušení položili jsme $x_1^2 = u$ a $x_2^2 = v$.

Tak nalezli jsme skupinu rovnic:

$$\begin{aligned} z^2 + y^2 &= u^2, \\ z^2 - y^2 &= v^2; \end{aligned} \qquad \text{(I)}$$

v nich jsou všechna čísla mezi sebou relativně nesoudělná, y sudé, ostatní lichá.

Tyto rovnice musí vedle sebe existovati, má-li rovnice $x^4 + y^4 = z^4$ býti možnou.

Ze skupiny (I) určíme si hodnotu veličiny y^2

$$y^2 = u^2 - z^2 = z^2 - v^2,$$

čili

$$y^2 = (u + z)(u - z) = (z + v)(z - v).$$

Ježto y jest sudé, ostatní čísla lichá, můžeme položiti:

$$\begin{aligned} u + z &= 2mn \\ u - z &= 2pr \\ z + v &= 2mp \\ z - v &= 2nr \\ y^2 &= 4mnpr, \end{aligned} \qquad \text{z čehož:} \qquad \begin{aligned} u &= mn + pr \\ z &= mn - pr = mp + nr \\ v &= mp - nr \\ y^2 &= 4mnpr. \end{aligned}$$

Z této sestavy jest zřejmo, že čísla m, n, p a r musí býti mezi sebou relativně nesoudělná, ježto čísla u, z, v a y jsou také mezi sebou relativně nesoudělná. (Kdyby na př. čísla m a n měla společného dělitele, musila by jej míti také čísla z a v; podobně musil by společný dělitel čísel m a r objeviti se také při číslech u, z a v atd.)

Z rovnice $y^2 = 4mnpr$ pak seznáváme, že relativně nesoudělná čísla m, n, p a r musí nutně býti kvadráty: tedy $m = y_1^2$, $n = y_2^2$, $p = y_3^2$, $r = y_4^2$ a $y^2 = 4y_1^2y_2^2y_3^2y_4^2$.

Vložme nyní hodnoty tyto do hořejších rovnic:

$$\begin{aligned} u &= y_1^2y_2^2 + y_3^2y_4^2 \\ z &= y_1^2y_2^2 - y_3^2y_4^2 = y_1^2y_3^2 + y_2^2y_4^2 \\ v &= y_1^2y_3^2 - y_2^2y_4^2 \end{aligned}$$

Pozorujeme-li druhou z těchto rovnic

$$y_1^2y_2^2 - y_3^2y_4^2 = y_1^2y_3^2 + y_2^2y_4^2$$

přepsanou ve tvarech:

$$y_1^2 (y_2^2 - y_3^2) = y_4^2 (y_2^2 + y_3^2)$$
a
$$y_2^2 (y_1^2 - y_4^2) = y_3^2 (y_1^2 + y_4^2),$$

shledáme, ježto y_1, y_2, y_3 a y_4 jsou mezi sebou relativně nesoudělná, že

$$y_2^2 + y_3^2 = sy_1^2 \quad \text{a} \quad y_1^2 + y_4^2 = ty_2^2$$
$$y_2^2 - y_3^2 = sy_4^2 \qquad\quad y_1^2 - y_4^2 = ty_3^2,$$

z čehož snadno vypočteme, že $st = 2$ čili, že z čísel s a t jedno jest jedničkou, druhé dvojkou.

Pro další řešení předpokládejme, že $t = 1$ (kdo chceš, vol $s = 1$), pak platí:

$$y_1^2 + y_4^2 = y_2^2,$$
$$y_1^2 - y_4^2 = y_3^2.$$

Z relativně nesoudělných veličin y_1, y_2, y_3 a y_4 musí tři býti liché, čtvrtá jest sudou, ježto ani součet ani rozdíl dvou lichých veličin nemůže býti lichým. Číselná forma kvadratických veličin nám pak snadno ukáže, že sudým musí býti y_4. (y_2 ani y_3 nemohou býti sudé, poněvadž by musily býti sudými současně obě — y_2^2 jest součtem, y_3^2 rozdílem týchž dvou čísel — jsou však mezi sebou relativně nesoudělná; y_1 nemůže také býti sudé, poněvadž číselná forma druhé rovnice $y_1^2 - y_4^2 = y_3^2$ — číselně $4h - 4k - 1 = 4l + 1$ čili $2d = 1$ — tomu odporuje.)

Tak dospěli jsme z původní skupiny (I) ke skupině nové

$$y_1^2 + y_4^2 = y_2^2, \qquad \text{(II)}$$
$$y_1^2 - y_4^2 = y_3^2,$$

v níž všechny veličiny y_1, y_2, y_3 a y_4 jsou faktory čísla $\frac{1}{2}y$.

Obě tyto skupiny mají stejné vlastnosti. Tam z, y, u a v jsou relativně nesoudělná, y sudé, ostatní čísla lichá, zde y_1, y_2, y_3 a y_4 také relativně nesoudělná, y_4 sudé, ostatní čísla lichá.

Týž postup, jaký jsme provedli na skupině (I), můžeme provésti též na skupině (II). Tím dospějeme k nové skupině

$$y_5^2 + y_8^2 = y_6^2, \qquad \text{(III)}$$
$$y_5^2 - y_8^2 = y_7^2,$$

v níž $\frac{1}{2}y_4 = y_5 y_6 y_7 y_8$; y_5, y_6, y_7, y_8 jsou mezi sebou relativně nesoudělná, y_8 sudé, y_5, y_6 a y_7 čísla lichá (podle téže úvahy jako nahoře).

Pokračujeme-li tímto způsobem, dojdeme k dalším skupinám (IV), (V) atd. Dělíme vždy číslo stojící uprostřed skupinových rovnic (y, y_4, y_8 atd.) dvěma a z kvocientu vzniknou nové čtyři faktory (mezi sebou relativně nesoudělné) jakožto veličiny tvořící další skupinu, z nichž vždy tři jsou lichými a jedna (prostřední) sudou. Ve tvoření nových skupin můžeme tedy pokračovati in inf.