4.6. Prvočísla Sophie Germainové

Základní vlastnosti. V roce 1819 se francouzská matematička Marie-Sophie Germainová proslavila částečným důkazem tzv. prvního případu Velké Fermatovy věty (srov. větu 4.20), tj. rovnice $x^p+y^p=z^p$ nemá řešení v přirozených číslech pro prvočíselný exponent $p > 2$ takový, že p nedělí součin xyz. Dokázala, že pokud p a $2p+1$ jsou současně prvočísly, pak první případ Velké Fermatovy věty platí pro exponent p.

Liché prvočíslo p, pro něž $2p + 1$ je také prvočíslem, se proto nazývá *prvočíslo Sophie Germainové.* Jsou to například prvočísla 5, 11 a 23.

Tato prvočísla mají řadu zajímavých vlastností. Je-li kupříkladu p prvočíslo Sophie Germainové, pak v (Křížek, Somer, 2001) dokazujeme, že všechna kvadratická nerezidua jsou primitivní kořeny modulo $2p + 1$ kromě jediného čísla $2p$, které je kvadratickým nereziduem, ale není primitivním kořenem. K této vlastnosti se ještě vrátíme ve větě 4.28.

Další věta, kterou znal již Fermat, ukazuje úzkou souvislost mezi Mersennovými čísly a prvočísly Sophie Germainové. Byla dokázána později Leonhardem Eulerem a nezávisle též Josephem Louisem Lagrangem.

Věta 4.22. *Nechť p je prvočíslo takové, že $p \equiv 3 \pmod 4$. Pak $2p + 1$ dělí Mersennovo číslo M_p právě tehdy, když $2p + 1$ je prvočíslo.*

Důkaz je uveden například v (Ribenboim, 1996, s. 90–91) a (Robbins, 1993, s. 149). Jestliže tedy $p = 11, 23, 83, \ldots$, pak M_p má prvočinitele 23, 47, 167, ... Další souvislost Mersennových prvočísel s prvočísly Sophie Germainové uvedeme ve větě 4.27.

Dosud nevíme, zda existuje nekonečně mnoho prvočísel Sophie Germainové. Pokud by existovalo nekonečně mnoho prvočísel Sophie Germainové p, pro něž $p \equiv 3 \pmod 4$, pak by také podle věty 4.22 existovalo nekonečně mnoho složených Mersennových čísel, neboť $2p + 1$ dělí $2^p - 1$.

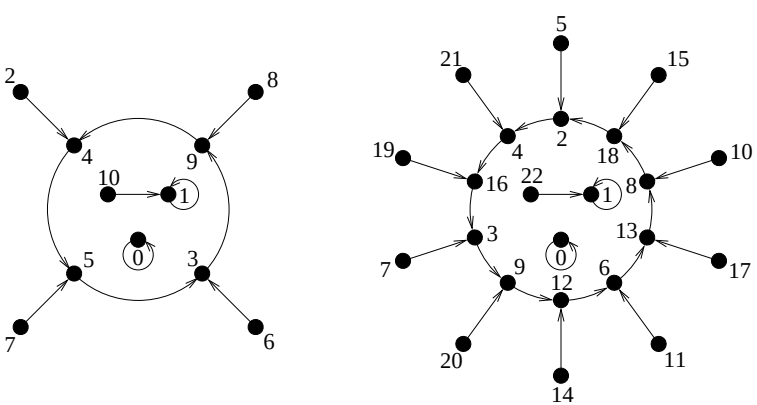
Pokud má množina prvočísel Sophie Germainové určitou hustotu, pak existuje deterministický polynomický algoritmus šestého stupně, který zjistí, zda je dané číslo prvočíslem, viz (Agrawal, Kayal, Saxena, 2004). Pro praktické účely je ale třeba najít algoritmus, který je nejvýše kubický[2)] v čase, jinak se dále budou pro testování prvočíselnosti používat pravděpodobnostní algoritmy založené na Malé Fermatově větě 2.13.

Největší známé prvočíslo Sophie Germainové do roku 2007 bylo

$$p = 7068555 \cdot 2^{121301} + 1,$$

tj. $2p + 1$ je také prvočíslo.

Struktura iteračních grafů. Pro každé přirozené číslo n uvažujme orientovaný graf $G(n)$ s vrcholy $0, 1, 2, \ldots, n-1$, jehož definice je stejná jako v oddílu 4.2, viz (4.11). Ukážeme, že když p je prvočíslo Sophie Germainové, pak má graf $G(2p+1)$ velice zajímavou strukturu. Jeho netriviální komponenty budou totiž připomínat sluníčka nebo kormidelní kolo, jímž se řídí loď – viz (Rogers, 1996, s. 323) a obrázky 4.13, 4.14 a 4.15.

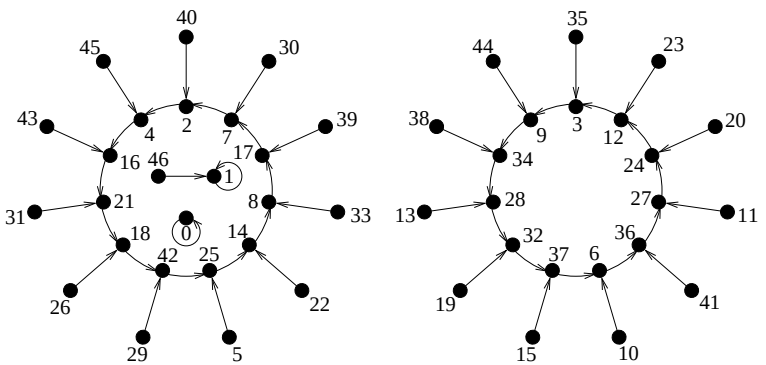


Obr. 4.13. Iterační orientované grafy odpovídající $n = 11$ a $n = 23$.

[2)] Pokud je pro zjištění prvočíselnosti daného čísla o n cifrách zapotřebí řádově n^3 aritmetických operací, pak se algoritmus nazývá *kubický*.

V práci (Rogers, 1996) se popisuje struktura každé komponenty grafu $G(n)$, je-li n prvočíslo. V článcích (Křížek, Somer, 2004) a (Somer, Křížek, 2004, 2006, 2007) vyšetřujeme strukturu $G(n)$ i pro n složená.

Nechť $\omega(n)$ označuje počet různých prvočísel, která dělí n. V příspěvku (Szalay, 1992) se dokazuje, že počet pevných bodů grafu $G(n)$ je roven $2^{\omega(n)}$. To vede k následujícímu tvrzení (srov. obr. 4.13 a 4.14).



Obr. 4.14. Iterační graf pro $n = 47$.

Věta 4.23. *Jestliže n je prvočíslo, pak existují právě dva pevné body grafu $G(n)$, totiž* 0 *a* 1.

Následující tvrzení jsou převzata z článku (Křížek, Somer, 2004). Využívají vlastností Carmichaelovy funkce λ, viz oddíl 2.8.

Věta 4.24. *V grafu $G(n)$ existuje cyklus délky t právě tehdy, když $t = \mathrm{ord}_d 2$ pro nějaký lichý kladný dělitel d čísla $\lambda(n)$.*

D ů k a z. Předpokládejme, že a je vrchol t-cyklu v $G(n)$. Pak t je nejmenší přirozené číslo, pro něž

$$a^{2^t} \equiv a \pmod{n}.$$

Odtud plyne, že t je nejmenší přirozené číslo, pro které

$$a^{2^t} - a \equiv a\left(a^{2^t-1} - 1\right) \equiv 0 \pmod{n}. \tag{4.17}$$

Protože $(a, a^{2^t-1} - 1) = 1$, ze vztahu (4.17) plyne, že když $n_1 = (a, n)$ a $n_2 = n/n_1$, pak t je nejmenší přirozené číslo takové, že

$$\begin{aligned} a &\equiv 0 \pmod{n_1}, \\ a^{2^t-1} &\equiv 1 \pmod{n_2}. \end{aligned} \tag{4.18}$$

Tudíž $(n_1, n_2) = 1$ a podle Čínské věty o zbytcích 1.4 dostaneme existenci celého čísla b takového, že

$$\begin{aligned} b &\equiv 1 \pmod{n_1}, \\ b &\equiv a \pmod{n_2}. \end{aligned} \tag{4.19}$$

Z výrazů (4.18) a (4.19) dále plyne, že t je nejmenší přirozené číslo, pro něž

$$b^{2^t-1} \equiv 1 \pmod{n}. \tag{4.20}$$

Nechť $d = \mathrm{ord}_n b$. Pak $d \mid \left(2^t - 1\right)$. Protože podle (4.20) je t nejmenší přirozené číslo, pro něž $d \mid \left(2^t - 1\right)$, vidíme, že $t = \mathrm{ord}_d 2$. Zřejmě je d liché, neboť $d \mid \left(2^t - 1\right)$. Navíc $d \mid \lambda(n)$, jak plyne z Carmichaelovy věty 2.20, protože podle (4.20) platí $(b, n) = 1$.

Předpokládejme obráceně, že d je lichý kladný dělitel $\lambda(n)$ a nechť $t = \mathrm{ord}_d 2$. Podle Carmichaelovy věty 2.20 existuje zbytek g modulo n tak, že $\mathrm{ord}_n g = \lambda(n)$. Nechť $h = g^{\lambda(n)/d}$. Pak $\mathrm{ord}_n h = d$. Jelikož $d \mid \left(2^t - 1\right)$ (ale $d \nmid \left(2^k - 1\right)$, kdykoliv $1 \leq k < t$), vidíme, že t je nejmenší přirozené číslo, pro které platí

$$h^{2^t-1} \equiv 1 \pmod{n}. \tag{4.21}$$

Potom

$$h \cdot h^{2^t-1} = h^{2^t} \equiv h \pmod{n},$$

a tedy h je vrcholem v t-cyklu $G(n)$. □

Věta 4.25. *Nechť p je prvočíslo Sophie Germainové. Pak $G(2p+1)$ má dvě triviální komponenty: izolovaný pevný bod 0 a komponentu $\{1, 2p\}$, jejíž pevný bod je 1. Každá ostatní komponenta má $2t$*

vrcholů a obsahuje t-cyklus, kde $t = \mathrm{ord}_p 2$. *Počet orientovaných hran přicházejících do každého z vrcholů t-cyklu je právě* 2.

D ů k a z. Protože $n = 2p + 1$ je prvočíslo, podle definice Carmichaelovy lambda funkce (viz oddíl 2.8) dostáváme

$$\lambda(2p + 1) = 2p.$$

Číslo $2p$ má právě dva liché dělitele 1 a p. Položíme-li $d = 1$ ve větě 4.24, dostaneme podle věty 4.23, že existují právě dva pevné body 0 a 1. Zřejmě 0 je jediné řešení kongruence $x^2 \equiv 0 \pmod{n}$, a tedy 0 je izolovaný pevný bod. Navíc $x = 1$ a $x = 2p$ jsou jediná řešení kongruence $x^2 \equiv 1 \pmod{n}$, neboť n je prvočíslo. Máme ukázat, že odpovídající komponenta obsahující $\{1, 2p\}$ nemá žádné jiné vrcholy. Protože p a n jsou lichá čísla, vidíme, že $n \equiv 3 \pmod 4$. Tedy $2p$ není kvadratický zbytek modulo n, což znamená, že kongruence $x^2 \equiv 2p \pmod{n}$ nemá řešení.

Položme nyní $d = p$ ve větě 4.24. Každá další komponenta $G(2p+1)$ tedy obsahuje cyklus délky $t = \mathrm{ord}_p 2$ pro $t > 1$. Jestliže vrchol a patří do tohoto t-cyklu, pak kongruence $x^2 \equiv a \pmod{n}$ má řešení, a tudíž a je kvadratický zbytek modulo n. Protože n je liché prvočíslo, má tato kongruence právě dvě řešení c a $-c$. Jedno z nich leží na t-cyklu a druhé mimo něj. Jelikož $n = 2p + 1 \equiv 3 \pmod 4$, jeden ze zbytků c nebo $-c$ musí být kvadratické reziduum a ten druhý kvadratické nereziduum modulo n.

Předpokládejme, že c není kvadratický zbytek modulo n. Pak c leží mimo t-cyklus a orientovaná hrana vycházející z c vstupuje do a. Protože c není kvadratický zbytek modulo n, neexistuje hrana vstupující do c. Proto má příslušná komponenta právě $2t$ vrcholů.

□

V článku (Křížek, Somer, 2004) se zabýváme též obrácenou větou 4.25.

Je-li p prvočíslo Sophie Germainové, pak všechny komponenty grafu $G(2p + 1)$, které neobsahují vrcholy 0 a 1, budeme nazývat *sluníčka Sophie Germainové.*

Jako důsledek dostáváme tuto větu.

Věta 4.26. *Nechť p je prvočíslo Sophie Germainové. Pak počet sluníček Sophie Germainové grafu $G(2p+1)$ je roven*

$$\frac{p-1}{\mathrm{ord}_p 2}. \tag{4.22}$$

D ů k a z. Z věty 4.25 víme, že počet vrcholů grafu $G(2p+1)$, které leží mimo triviální komponenty, je roven $2p-2$. Podle věty 4.25 každé sluníčko Sophie Germainové má $2\,\mathrm{ord}_p 2$ vrcholů, což dokazuje tvrzení. □

Poznámka. Jestliže $2p+1$ je prvočíslo a $p > 1$, pak $2p-2$ není dělitelné 3. Tudíž podle (4.22) není počet sluníček Sophie Germainové nikdy dělitelný 3 a délka všech příslušných t-cyklů také není dělitelná 3.

Nyní dokážeme poněkud obecnější tvrzení, a to, že $G(2p+1)$ nikdy neobsahuje q-cyklus pro $q = 3, 5, 7, 13, 17, 19, \ldots$, což jsou exponenty všech Mersennových prvočísel $M_q = 2^q - 1$ s $q > 2$. (Poznamenejme, že $G(7)$ obsahuje 2-cyklus.)

Věta 4.27. *Nechť M_q je Mersennovo prvočíslo pro $q > 2$. Pak neexistuje prvočíslo Sophie Germainové p tak, že $G(2p+1)$ obsahuje q-cyklus.*

D ů k a z. Předpokládejme naopak, že existuje prvočíslo Sophie Germainové p a Mersennovo prvočíslo M_q pro $q > 2$ tak, že $G(2p+1)$ obsahuje q-cyklus. Pak podle věty 4.25 je $q = \mathrm{ord}_p 2$, a tudíž $p = 2^q - 1$. Číslo

$$2p + 1 = 2^{q+1} - 1 = (2^{(q+1)/2} + 1)(2^{(q+1)/2} - 1)$$

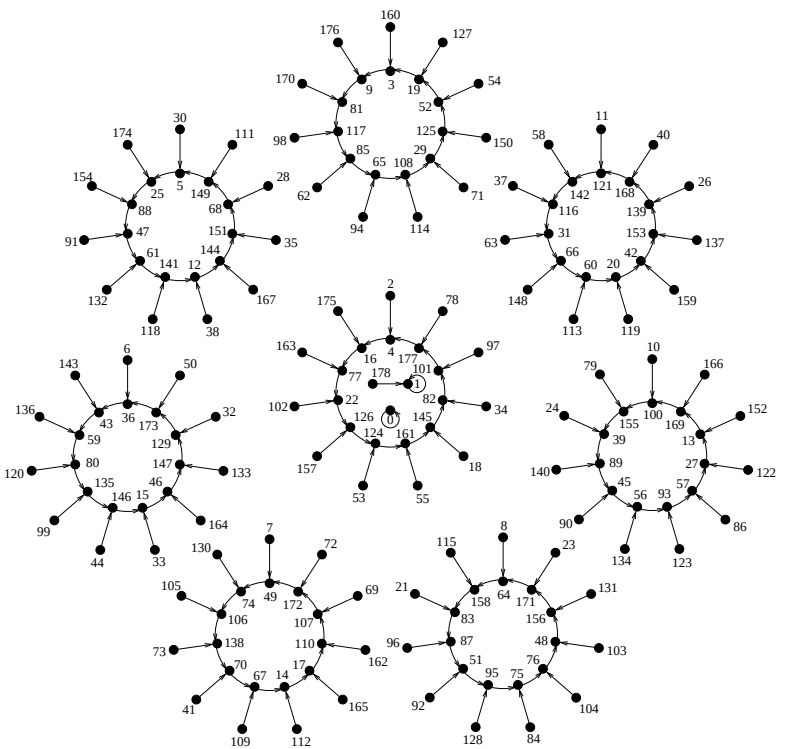
je ale složené pro prvočíslo $q > 2$, což je spor. □

Toto tvrzení tedy opět svazuje Mersennova prvočísla s prvočísly Sophie Germainové.

Příklad. Nechť $p = 89$. Protože $2^{11} \equiv 1 \pmod{89}$, vidíme, že $\mathrm{ord}_{89} 2 = 11$. Tudíž podle věty 4.26 počet sluníček Sophie Germainové grafu $G(179)$ je $88/11 = 8$ (obr. 4.15).

Poznamenejme ještě, že orientované grafy $G(n)$ odpovídající Mersennovým číslům n se vyšetřují v článku (Szalay, 1992). V článcích (Somer, Křížek, 2006, 2007) vyšetřujeme strukturu orientovaných grafů odpovídající kongruenci $f(x) \equiv x^k \pmod{n}$ pro $k \geq 2$, která je obecnější než (4.11).

Z věty 4.16 víme, že počet primitivních kořenů Fermatových prvočísel je roven počtu kvadratických nereziduí. Jiná prvočísla tuto vlastnost nemají. Předpokládejme nyní, že p je prvočíslem Sophie Germainové. Následující věta ukazuje, že počet primitivních kořenů prvočísla $2p + 1$ je jen o jednu menší než počet kvadratických nereziduí, kterých je p.



Obr. 4.15. Iterační orientovaný graf pro $n = 179$.