Сава Гроздев
БАН, Софија

МИНИМАЛЕН ПРОСТ ДЕЛИТЕЛ

Согласно основната теорема на аритметиката, секој природен број n може да се претстави во облик:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \qquad (1)$$

каде што $p_1, p_2, \dots, p_k$ се сите различни прости делители на бројот n, а α_i е највисокиот степен на p_i така што $p_i^{\alpha_i}$ го дели n. Изразот (1) се нарекува канонично разложување на бројот n. Во теоријата на деливоста на природните броеви, која што популарно ја нарекуваме елементарна теорија на броеви, често се бара брзо наоѓање на остатокот од делењето на високи степени на природен број со друг природен број. Во такви случаи корисна е така наречената мала теорема на Ферма (Пјер Ферма (1601-1665)), според која

$$a^{p-1} \equiv 1 \pmod{p}, \qquad (2)$$

каде што p е прост број, а бројот a не се дели со p.

И покрај тоа што малата теорема на Ферма е корисна во многу конкретни ситуации, таа е недоволна за решавање на проблеми од таков тип. Поопшто тврдење од неа е така наречената теорема на Ојлер (Леонард Ојлер (1707-1783)). Ојлер забележал, дека степенот $p-1$ во (2) е точно бројката на броеви, кои се помали од p и се заемно прости со p. Ојлер за произволен природен број n тој број го означил со $\varphi(n)$, т.е. $\varphi(n)$ е бројката на броеви кои што се помали од n и се заемно прости со n. Ако n не е прост број, тогаш јасно е дека $\varphi(n) < n-1$. Јасно е исто така дека $\varphi(1) = 1$. На тој начин, φ станува функција определена на множеството природни броеви и која прима вредности исто така во множеството природни броеви. Општо прифатено е таа функција да се нарекува Ојлерова функција, според името на нејзиниот творец. Со помош на оваа функција, Ојлер ја обопштил малата теорема на Ферма, и обопштената теорема се нарекува теорема на Ојлер. Според таа теорема

$$a^{\varphi(n)} \equiv 1 \pmod{n} \qquad (3)$$

каде што a и n се заемно прости природни броеви.

Ојлеровата функција има многу интересни и важни својства. Некои од нив ќе ги споменеме во наредниот дел.

Теорема 1. Ојлеровата функција е мултипликативна, т.е.

$$\varphi(mn) = \varphi(m)\varphi(n)$$

за произволни заемно прости природни броеви n и m.

Доказот на ова тврдење нема да го разгледуваме, но ќе ја забележиме следната последица од неа, која лесно се докажува со индукција:

Последица 1. Ако $m_1, m_2, ..., m_k$ се попарно заемно прости броеви, тогаш

$$\varphi(m_1 m_2 ... m_k) = \varphi(m_1)\varphi(m_2)...\varphi(m_k) \qquad (4)$$

Теорема 2. Ако n е природен број и $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ е неговото канонично разложување (1), тогаш

$$\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k}) . \qquad (5)$$

Доказ. Во случајот $n = p^{\alpha}$, каде што p е прост број, броевите $p, 2p, 3p, ..., p^{\alpha-1}\cdot p$ се единствените кои не се взаемно прости со p^{α} и не се поголеми од него. Нивниот број е $p^{\alpha-1}$. Според тоа взаемно простите броеви со бројот p^{α} и кои се помали од него ги има $p^{\alpha} - p^{\alpha-1}$. Според тоа, во овој случај

$$\varphi(n) = \varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}(1-\frac{1}{p}) = n(1-\frac{1}{p}) .$$

Со тоа во овој случај тврдењето од теоремата е докажано.

За доказот на општиот случај ќе ја искористиме последицата од теорема 1. Според неа:

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})...\varphi(p_k^{\alpha_k}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1})...(p_k^{\alpha_k} - p_k^{\alpha_k-1}) \\ &= p_1^{\alpha_1}(1-\frac{1}{p_1}) p_2^{\alpha_2}(1-\frac{1}{p_2})...p_k^{\alpha_k}(1-\frac{1}{p_k}) \\ &= n(1-\frac{1}{p_1}) p_2^{\alpha_2}(1-\frac{1}{p_2})...(1-\frac{1}{p_k})\end{aligned}$$

Со тоа (5) е докажано.

Во натамошниот тек на изложувањата ќе имаме потреба од следната дефиниција.

Дефиниција 1. Ако a и n се заемно прости броеви, тогаш најмалиот природен број k за кој $a^k \equiv 1 \pmod{n}$, се нарекува степен на a по модул n.

Да забележиме дека множеството од броеви m за кои $a^m \equiv 1 \pmod{n}$ не е празно. Од теоремата на Ојлер следува дека бројот $\varphi(n)$ припаѓа на тоа множество. Според тоа дефиницијата 1 е оправдана и коректна. Во специјален случај, кога n е прост број, коректноста следува од малата теорема на Ферма.

Теорема 3. Ако a и n се заемно прости природни броеви и k е степен на a по модул n, тогаш $a^m \equiv 1 \pmod{n}$ за некој природен број тогаш и само тогаш кога k го дели m.

Доказ. Ако k го дели m, тогаш $m = qk$ за некој природен број q. Бидејќи $a^k \equiv 1 \pmod{n}$, добиваме $a^{qk} \equiv 1^q \pmod{n}$ па според тоа $a^m \equiv 1 \pmod{n}$.

Обратно, нека $a^m \equiv 1 \,(\mathrm{mod}\, n)$ и $m = qk + r$, каде што r е остатокот од делењето на m со k. Според тоа $0 \le r \le k-1$. Бидејќи $a^{qk+r} \equiv 1 \,(\mathrm{mod}\, n)$, добиваме $a^{qk}a^r \equiv 1 \,(\mathrm{mod}\, n)$. Од условот на теоремата $a^k \equiv 1 \,(\mathrm{mod}\ n)$, т.е. $a^{qk} \equiv 1 \,(\mathrm{mod}\ n)$. Според тоа $a^r \equiv 1 \,(\mathrm{mod}\ n)$. Конечно добиваме $r = 0$, бидејќи во спротивен случај добиваме контрадикција со минималноста на k. Значи, бројот k го дели бројот m. \

Досегашните разгледувања се доволни за решавање на низа содржајни задачи.

Задача 1. Да се најдат сите природни броеви n, за кои бројот $\frac{n}{\varphi(n)}$ е исто така природен број.

Решение. Нека $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ е каноничната репрезентација (1) на n. Од (5) заклучуваме дека

$$\frac{n}{\varphi(n)} = \frac{p_1 p_2 \cdots p_k}{(p_1-1)(p_2-1)\dots(p_k-1)}.$$

Без ограничување на општоста можеме да претпоставиме дека $p_1 < p_2 < \dots < p_k$. Ако $k \ge 3$, тогаш $p_2 \ne 2$ па според тоа бројот $p_2 - 1$ е парен број. Бидејќи $p_3, p_4, \dots, p_k$ се прости броеви, секој од броевите $p_3 - 1, p_4 - 1, \dots, p_k - 1$ се парни броеви. Значи именителот на $\frac{n}{\varphi(n)}$ се дели со 2^{k-1} и според тоа и со 2^2 бидејќи $k \ge 3$. Од друга страна броителот се дели најмногу со 2, и тоа во случај кога $p_1 = 2$. Според тоа, за бараните броеви n од задачата, $k = 1$ или $k = 2$.

При $k = 1$ мора да е исполнет условот $p_1 = 2$, бидејќи во спротивно именителот на $\frac{p_1}{p_1-1}$ се дели со 2, а броителот би бил непарен број. Според тоа $\frac{p_1}{p_1-1}$ не е цел број. Решение на задачата во случајот $k = 1$ се сите цели броеви n од облик $n = 2^{\alpha}$, каде α е произволен природен број.

При $k = 2$, со аналогни разгледувања како и во претходниот дел, се покажува дека $p_1 = 2$. Ќе покажеме дека $p_2 = 3$. Да претпоставиме спротивно, т.е. дека $p_2 > 3$. Тогаш $p_2 = 2q + 1$, каде $q > 1$. За количникот $\frac{n}{\varphi(n)}$ добиваме

$$\frac{n}{\varphi(n)} = \frac{2 \cdot p_2}{1 \cdot 2 \cdot q} = \frac{p_2}{q}.$$

За да бројот $\frac{p_2}{q}$ биде цел број, мора да е исполнет $q = 1$ бидејќи p_2 е прост број поголем од 3 а $q < 1$. Во тој случај $p_2 = 3$ што е во спротивност со почетната претпоставка. Значи $p_2 = 3$.

Конечно, бараните броеви имаат облик $n=2^{\sim}3$, каде ~ и се произволни природни броеви. Да напоменеме дека може да прима вредност 0 .

Во решението на претходната задача суштински е тоа што бројот 2 е минимален прост делител на бројот n. Во натамошните примери се користи идејата за минимален прост делител, од каде што доаѓа и насловот на оваа статија.

Задача 2. (Романска олимпијада). Да се најдат сите природни броеви n , за кои што $\frac{2^n-1}{n}$ е исто така природен.

Решение. Очигледно е дека $n=1$ не е решение. Нека $n\geq 2$. Случајот кога 2 го дели n не е можен, бидејќи броевите 2 и 2^n-1 се взаемно прости. Наместо 2 , како што направивме во претходната задача, нека p е минималниот прост делител на n . Во тој случај, за да бројот $\frac{2^n-1}{n}$ е цел број, потребно е бројот p да го дели бројот 2^n-1. Нека k е степенот на 2 по модул p. Од теорема 3 добиваме дека k го дели n . Според малата теорема на Ферма, $2^{p-1}\equiv 1(\bmod\ p)$ и тогаш повторно според теорема 3, добиваме дека k го дели $p-1$. Значи заклучивме дека k ги дели броевите n и $p-1$, па според тоа и нивниот најголем заеднички делител.

Дефиниција 2. Ако a, b и n се природни броеви, за кои како a и n , така и b и n се заемно прости, тогаш најмалиот природен број k за кој $a^k\equiv b^k\ (\bmod\ n)$ се нарекува степен на a и b по модул n .

Да забележиме дека, согласно теоремата на Ојлер $a^{¨(n)}\equiv 1(\bmod n)$ и $b^{¨(n)}\equiv 1(\bmod n)$, па според тоа $a^{¨(n)}-b^{¨(n)}\equiv 0(\bmod n)$. Значи, горната дефиниција е коректна. На аналоген начин се определува степен на повеќе броеви кои се взаемно прости со даден природен број n .

Теорема 4. Ако a, b и n се природни броеви, за кои како a и n така и b и n се взаемно прости, k е степенот на a и b по модул n, тогаш $a^m\equiv b^m\ (\bmod\ n)$ за некое m ако и само ако k го дели m .

Доказот е ист како во теорема 3.

Задача 3. Да се најдат сите природни броеви n за кои бројот $\frac{3^n-2^n}{n}$ е природен број.

Решение. Очигледно е дека $n=1$ е решение. Во наредниот дел ќе ги гледаме природните броеви кои поголеми или еднакви на 2 . Нека p е минималниот прост делител на n. Ако $\frac{3^n-2^n}{n}$ е цел број, тогаш p го дели 3^n-2^n, па според тоа $p\neq 2$ и $p\neq 3$. Нека k е степенот на 2 и 3 по модул p. Според теорема 4 k го дели n. Од друга страна, според малата теорема на Ферма $3^{p-1}\equiv 1(\mod p)$ и $2^{p-1}\equiv 1(\mod p)$. Одново, со помош на теорема 4 добиваме дека k го дели $p-1$. Според тоа $k\leq p-1$ и k истовремено ги дели n и $p-1$. Од минималноста на p, добиваме $k=1$. Значи $3^1\equiv 2^1 \ (\mod \ p)$, што не е можно.

Значи, единствено решение на задачата е $n=1$.

Задача 4. Да се најдат сите природни броеви m и n, за кои бројот $\frac{(m+1)^n-m^n}{n}$ е исто така природен.

Решение. Јасно е дека $n=1$ е решение на задачата, и заради тоа ќе разгледуваме случај $n\geq 2$. Нека p е минималниот прост делител на бројот n. Бројот $(m+1)^n-m^n$ е непарен како разлика на два броја со различна парност и ако бројот $\frac{(m+1)^n-m^n}{n}$ е цел, тогаш $p\neq 2$. Освен тоа броевите $m+1$ и m не се делат со p. Нека k е степенот на $m+1$ и m по модул p. Од теорема 4 добиваме дека k го дели n. Според малата теорема на Ферма $(m+1)^{p-1}\equiv 1(\mod \ p)$ и $m^{p-1}\equiv 1(\mod \ p)$, од каде што $(m+1)^{p-1}\equiv m^{p-1}(\mod \ p)$ и повторно според теорема 4 добиваме дека k го дели $p-1$. Како и во задача 3 добиваме дека k е делител на n и на $p-1$. Според тоа $k\leq p-1$ и од минималноста на p добиваме $k=1$. Според тоа $m+1\equiv m(\mod \ p)$, кое што е невозможно заради претпоставката за p.

Значи, единствено решение на задачата е $n=1$.

Природно обопштување на горната задача е да се најдат сите природни броеви m, l и n за кои бројот $\frac{(m+l)^n-m^n}{n}$ е природен. Бројот $\frac{(m+l)^n-m^n}{n}$ очигледно е природен при $n=1$ и произволни броеви m и l. Ако $n\neq 1$ тоа очигледно не е точно. Во наредната задача ќе го разгледаме случајот $n\neq 1$.

Задача 5. Да се докаже дека ако $m, n\neq 1$ и l се природни броеви за кои бројот $\frac{(m+l)^n-m^n}{n}$ е природен, тогаш минималниот прост делител на n го дели l.

Решение. Нека p е минималниот прост делител на n и да претпоставиме дека p не го дели l. Според условот на задачата $\frac{(m+l)^n-m^n}{n}$ е природен. Значи, p не го дели m, бидејќи во спротивен случај p ќе го дели

$$(m+l)^n = m^n + n\cdot m^{n-1}\cdot l + \frac{n(n-1)}{2} m^{n-2} l^2 + ... + n\cdot m\cdot l^{n-1} + l^n ,$$

од каде следува дека p го дели l^n, па според тоа p го дели l, што е во спротивност со претпоставката. Значи p не го дели m. Од истите причини p не го дели ни $m+l$. Значи, конечно p не е делител ни на m ни на $m+l$. Нека k е степенот на $m+l$ и m по модул p. Како и во претходната задача со помош на теорема 4 и малата теорема на Ферма заклучуваме дека $k=1$. Тогаш $m+l \equiv m(\mathrm{mod}\ \ l)$, т.е. $l \equiv 0(\mathrm{mod}\ \ l)$, кое противречи на претпоставката.

Задача 6. (Материјали на жирито од Меѓународната олимпијада од 1990) Да се најдат сите природни броеви n, за кои $\frac{2^n+1}{n^2}$ е исто така природен број.

Решение. Задачата е романски предлог и нејзин автор е раководителот на Романскиот национален комитет за Меѓународната олимпијада во Кина во 1990 г., проф. Јоан Томеску.

Јасно е дека $n=1$ е решение на задачата. Нека n е природен број поголем од еден и нека тој е решение на задачата. Ако p е минималниот прост делител на n, тогаш $p \neq 2$, бидејќи во спротивен случај $\frac{2^n+1}{p^2}$ е природен број што не е точно. Значи $p \geq 3$. Ако $\frac{2^n+1}{n^2}$ е природен број, тогаш бројот $\frac{2^n+1}{n}$ е исто така природен број. Значи, природниот број n го дели бројот 2^n+1. Во тој случај бројот n го дели и бројот $(2^n+1)(2^n-1) = 4^n - 1$, т.е. бројот $\frac{(1+3)^n-1}{n}$ е природен број. Од задача 5 добиваме дека p е делител на 3. Бидејќи p е прост број, добиваме $p=3$. Нека $n = 3^m \cdot l$, каде m и l се природни броеви и 3 не го дели l. Јасно е дека $m \geq 1$. Ќе покажеме дека $m=1$.

Нека претпоставиме спротивно, т.е. дека $m \geq 2$. Тогаш

$$\begin{aligned} 2^n+1 = 2^{3^m\cdot l}+1 &= (2^{3^{m-1}\cdot l})^3 + 1^3 = (2^{3^{m-1}\cdot l}+1)(2^{2\cdot 3^{m-1}\cdot l} - 2^{3^{m-1}\cdot l}+1) \\ &= ((2^{3^{m-2}\cdot l})^3 + 1^3)(2^{2\cdot 3^{m-1}\cdot l} - 2^{3^{m-1}\cdot l}+1) \\ &= (2^{3^{m-2}\cdot l}+1)(2^{2\cdot 3^{m-2}\cdot l} - 2^{3^{m-2}\cdot l}+1)(2^{2\cdot 3^{m-1}\cdot l} - 2^{3^{m-1}\cdot l}+1) \end{aligned}$$

и ако продолжиме на истиот начин ќе добиеме дека

$$2^n+1 = (2^l+1)\prod_{j=0}^{m-1}(2^{2\cdot 3^j\cdot l} - 2^{3^j\cdot l}+1) \tag{6}$$

Но

$$2^{2\cdot 3^j\cdot l} = 4^{3^j\cdot l} = (3+1)^{3^j\cdot l} = 3^{3^j\cdot l} + 3^j\cdot l\cdot 3^{3^j\cdot l-1} + ... + 3^j\cdot l\cdot 3 + 1 \equiv 1(\mathrm{mod}\ \ 9)$$

за секој $j = 1,2,...,m-1$. Освен тоа, за секој $j = 1,2,...,m-1$ имаме

$$2^{3^j\cdot l}=(3-1)^{3^j\cdot l}=3^{3^j\cdot l}-3^j\cdot l\cdot 3^{3^j\cdot l-1}+\ldots+3^j\cdot l\cdot 3-1\equiv -1(\bmod\ 9)$$

бидејќи l е непарен. Значи $2^{2\cdot 3^j\cdot l}-2^{3^j\cdot l}+1\equiv 3(\bmod 9)$.

Аналогно како и претходно, за $j=0$, добиваме $2^{2l}-2^l+1\equiv 3(\bmod 9)$. Тогаш највисок степен на 3 во производот $\prod_{j=0}^{m-1}(2^{2\cdot 3^j\cdot l}-2^{3^j\cdot l}+1)$ е m. Значи, за да $(3^m l)^2$ го дели 2^n+1, потребно е 3^m да го дели 2^l+1. Ако $m\geq 2$, тогаш $4^l\equiv 1(\bmod\ 9)$. Но степенот на 4 по модул 9 е 3, и според теорема 3 добиваме дека 3 го дели l. Но тоа не е можно според почетната претпоставка од овој дел.

Значи $m=1$.

Нека $n=3l$ и 3 не е делител на l. Најмалиот прост делител q на l, бидејќи $\frac{2^n+1}{n^2}$ е природен број е делител и на 2^n+1, па според тоа е делител и на 4^n-1. Ако s е степенот на 4 по модул q, т.е. $4^s\equiv 1(\bmod\ q)$, тогаш според теорема 3 добиваме дека s го дели n. Од друга страна, според малата теорема на Ферма $4^{q-1}\equiv 1(\bmod\ q)$ и повторно според теорема 3 добиваме дека s го дели $q-1$, $s\leq q-1$. Од минималноста на q добиваме дека s го дели 3. Според тоа за s имаме две можности и тоа $s=1$ или $s=3$.

Ако $s=3$, тогаш $4^3\equiv 1(\bmod\ q)$. За простите броеви кои се поголеми од 64, очигледно последното не е можно. За простите броеви кои се помали од 64 и се различни од 3, само за $q=7$ е исполнето $64\equiv 1(\bmod\ 7)$. Но со диеректна проверка добиваме дека 7 не го дели $2^{21i}+1$.Непосредно се добива дека за секој природен број i, $2^{21i}+1\equiv 2(\bmod\ 7)$. Значи единствена можност е $s=1$. Но $4^1\equiv 1(\bmod\ q)$ е исполнето само при $q=3$. Тоа не е можно бидејќи l не се дели со 3. Конечно $l=1$.

Значи решенија на задачата се $n=1$ и $n=3$.

Статијата прв пат е објавена во списанието СИГМА на Сојузот на математичарите на Македонија