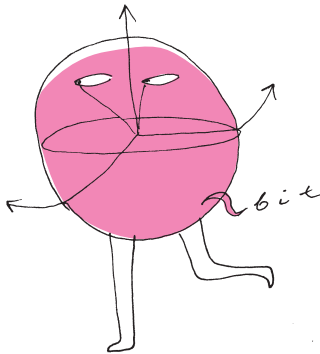


Komputery kwantowe – od Feynmana do Google’a

*Instytut Fizyki Teoretycznej, Wydział Fizyki, Uniwersytet Warszawski

Rafał DEMKOWICZ-DOBRZAŃSKI*

„Informacja jest fizyczna” powiedział Rolf Landauer, fizyk, któremu zawdzięczamy zrozumienie faktu, że usunięcie 1 bitu informacji z pamięci komputera wiąże się z nieuniknionym wytworzeniem ciepła o wartości $kT \ln 2$, gdzie T jest temperaturą otoczenia, a k stałą Boltzmanna. Był to wynik, który pokazał, że warto myśleć o fizycznych podstawach przetwarzanej przez nas informacji, aby zrozumieć ograniczenia i perspektywy dalszego rozwoju komputerów. Dziś wiemy, że materia na poziomie mikroskopowym opisywana jest przez prawa fizyki kwantowej. Pojawia się więc naturalne pytanie, jak fakt ten odbija się na naszych możliwościach przetwarzania informacji. Czy jest to bardziej przeszkoda, związana z rozmytą naturą stanów kwantowych, powodująca, że np. elektrony nie będą chciały pozostawać dobrze zlokalizowane w sytuacji zbyt daleko idącej miniaturyzacji obwodów elektrycznych, czy może daje to nadzieję na wykorzystanie potencjału układów kwantowych mogących być „w wielu stanach jednocześnie”, aby uzyskać niewyobrażalne w podejściu klasycznym zrównoleglenie obliczeń?



Warto podkreślić, że działanie dzisiejszych komputerów, które w żargonie informatyków kwantowych nazywa się klasycznymi, również oparte jest na prawach fizyki kwantowej. Pasmowa struktura półprzewodników wykorzystywana do produkcji układów scalonych jest makroskopową emanacją kwantowej natury atomów. Własności magnetyczne materii wykorzystywane do zapisu danych są ściśle związane z jedną z najbardziej kwantowych cech elementarnych składników materii, jaką jest spin. Niemniej, nawet przy obecnym postępie miniaturyzacji, na każdą elementarną bramkę logiczną w układach scalonych czy pojedynczy bit informacji zapisany w pamięci komputera przypada wciąż bardzo duża liczba atomów, rzędu miliona. Ten fakt powoduje, że tak naprawdę subtelne własności kwantowe materii nie są w pełni dostępne i kontrolowalne, więc z bardzo dobrym przybliżeniem przetwarzanie informacji w takim układzie można traktować w czysto klasyczny sposób.

Richard Feynman w swoich wizjach rozwoju komputerów mówił: „jest bardzo dużo miejsca tam na dole”, mając na myśli, że rozwijając nasze technologie wciąż pozostajemy na poziomie makroskopowym, nie wykorzystując w pełni potencjału oferowanego przez świat mikroskopowy. Stwierdzenie to, jak widać z powyższych rozważań, jest aktualne do dziś. Chciałoby się zbudować komputer operujący nie na układach milionów atomów, ale na pojedynczych atomach, wykorzystując do maksimum ich własności kwantowe – stworzyć komputer kwantowy.

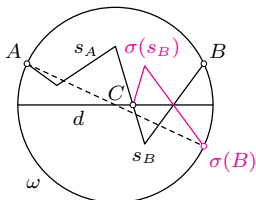
Bawiąc się w futurologię, można w zasadzie przewidzieć datę powstania komputera kwantowego. Od lat 70. obserwuje się stale postępującą miniaturyzację układów scalonych, powodującą, że gęstość upakowania elementarnych komponentów elektronicznych rośnie dwukrotnie w czasie mniej więcej 18 miesięcy. Obserwacja ta znana jest pod nazwą prawa Moore’a. Mimo pewnych obaw co do utrzymania tego trendu, obserwujemy go do dzisiaj. Jeśli wierzyć, że trend ten się utrzyma, można oszacować moment, kiedy miniaturyzacja układów doprowadzi do sytuacji, że pojedynczy tranzystor będzie rozmiarów pojedynczego atomu. Powinno to nastąpić około roku 2040.

W idei komputera kwantowego nie chodzi jednak tylko o zbudowanie urządzenia wykonującego klasyczne obliczenia na układach logicznych zbudowanych z pojedynczych atomów. W przypadku obliczeń klasycznych wartości bitów mogą przyjmować wartości 0 lub 1. Myśląc o kwantowym odpowiedniku bitu, czyli np. o atomie, w którym wartość 0 lub 1 będziemy zapisywać poprzez przygotowanie atomu w jeden z dwóch różnych stanów energetycznych $|0\rangle$, $|1\rangle$, musimy pamiętać, że zgodnie z kwantową zasadą superpozycji możemy również przygotować atom w dowolnej superpozycji tych dwóch stanów $|\psi\rangle = a|0\rangle + b|1\rangle$, gdzie a, b są liczbami zespolonymi spełniającymi warunek $|a|^2 + |b|^2 = 1$, tak aby $|\psi\rangle$ był wektorem o długości 1. Taki kwantowy bit mogący znajdować się w stanie będącym dowolną superpozycją $|0\rangle$ i $|1\rangle$ nazywamy *kubitem*. Dzięki



Rozwiązanie zadania M 1549.
Oznaczmy przez A, B końce łamanej s . Niech d będzie średnicą okręgu ω równoległą do AB . Udowodnimy, że d spełnia warunki zadania.

Przypuśćmy przeciwnie, czyli że łamana s ma ze średnicą d co najmniej jeden punkt wspólny C i oznaczmy fragmenty łamanej s od punktu A do punktu C oraz od punktu C do punktu B odpowiednio przez s_A oraz s_B .



Rozważmy symetrię σ względem prostej zawierającej d . Wówczas, skoro $AB \parallel d$, to odcinek $A\sigma(B)$ jest średnicą ω , wobec czego

$$1 = |A\sigma(B)| \leq |s_A| + |\sigma(s_B)| = |s_A| + |s_B| = |s| < 1,$$

gdzie $|s|$, $|s_A|$, $|s_B|$ oznaczają długości odpowiednich łamanych. Uzyskana sprzeczność kończy rozwiązanie zadania.

**Rozwiązanie zadania M 1550.**

Udowodnimy najpierw, że dla dowolnych dodatnich liczb rzeczywistych x, y oraz dodatniej liczby całkowitej k zachodzi nierówność

$$x^2 + ky^2 \geq \frac{k}{k+1}(x+y)^2.$$

Rzeczywiście, przekształcając tę nierówność równoważnie, otrzymujemy

$$x^2 + kx^2 + ky^2 + (ky)^2 \geq kx^2 + 2kxy + ky^2, \\ (x-ky)^2 \geq 0.$$

Przyjmując w powyższej nierówności $(x, y) = (a_{k-1}, a_k)$ dla $k = 1, 2, \dots, n$, mnożąc otrzymane związki stronami i korzystając z założenia zadania, uzyskujemy

$$\prod_{k=1}^n (a_{k-1}^2 + ka_k^2) \geq \\ \geq \prod_{k=1}^n \frac{k}{k+1} \cdot \prod_{k=1}^n (a_{k-1} + a_k)^2 = \\ = \frac{1}{n+1}.$$

Uwaga. Można sprawdzić, że równość w dowodzonej nierówności zachodzi wtedy i tylko wtedy, gdy

$$a_k = \frac{1}{k!} \sqrt{\prod_{i=1}^n i!}.$$

**Rozwiązanie zadania M 1551.**

Jeżeli n jest liczbą parzystą, to żądanym przedstawieniem jest $2n - n$.

Przypuśćmy, że n jest liczbą nieparzystą i niech p będzie najmniejszą nieparzystą liczbą pierwszą, która nie jest dzielnikiem liczby n . Wówczas przedstawienie liczby n w postaci różnicy

$$pn - (p-1)n$$

spełnia warunki zadania. Rzeczywiście, każda z liczb pn oraz $(p-1)n$ ma dokładnie te dzielniki pierwsze co liczba n , a ponadto po jednym dodatkowym — odpowiednio p oraz 2 .

zasadzie superpozycji, mając np. N kubitów, możemy przygotować stan będący równoczesną superpozycją stanów, które reprezentują wszystkie liczby N bitowe. (W modelu obliczeń reprezentujemy taką superpozycję przez wektor długości 1 z przestrzeni \mathbb{C}^{2^N} .) Dzięki temu możliwe jest wykonanie obliczeń równoległe na wszystkich składnikach superpozycji (poprzez przemnożenie wektora zawartości pamięci przez macierz unitarną) i uzyskanie przyspieszenia obliczeń niedostępnego w ramach klasycznego modelu obliczeń. Jest to fundamentalna idea leżąca u podłoża wszystkich algorytmów kwantowych, których działanie opisane jest bardziej szczegółowo w artykule o modelu obliczeń kwantowych na stronach 1–3.

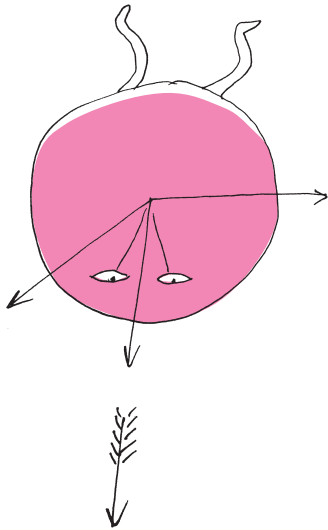
Jak więc zbudować komputer kwantowy? Pierwszą decyzją, jaką należy podjąć, jest wybór architektury obliczeń kwantowych. Najpopularniejszą, choć nie jedyną (popatrzmy chociażby na artykuł ze stron 12–15) architekturą, jest ta oparta o bramki kwantowe, które podobnie jak w podejściu klasycznym tworzą obwody logiczne realizujące obliczenia. W przypadku obliczeń klasycznych każdy obwód logiczny można zbudować z bramek typu NAND, których działanie polega na zamianie dwóch bitów wejściowych x_1, x_2 na jeden bit wyjściowy y w taki sposób, że $y = 0$, gdy $x_1 = x_2 = 1$, i $y = 1$ w pozostałych trzech przypadkach. Bramka NAND jest bramką nieodwracalną. Znając jedynie wartość bitu na wyjściu, w ogólności nie można odtworzyć wartości bitów wejściowych. Zwróćmy uwagę, że utrata jednego bitu informacji, która następuje podczas każdego użycia bramki NAND, zgodnie ze wspomnianą wcześniej zasadą Landauera musi wiązać się z wytworzeniem ciepła o wartości $kT \ln 2$. W przypadku obliczeń klasycznych możliwa jest modyfikacja bramek logicznych tak, by stały się odwracalne, poprzez przekazanie dodatkowych informacji do wyjścia bramki, unikając tym samym wytworzenia ciepła. Odbywa się to jednak kosztem komplikacji układu logicznego. Nie jest to obecnie stosowane w praktyce, gdyż energia $kT \ln 2$ jest wciąż o wiele rzędów wielkości niższa niż ciepło wydzielane w obecnie wykorzystywanych bramkach logicznych. W przypadku obliczeń kwantowych odwracalność obliczeń ma jednak kluczowe znaczenie. Nie chodzi tu jedynie o kwestię ciepła, ale o fakt, że utrata informacji o części układów kwantowych prowadzi w ogólności do tak zwanego zjawiska dekoherencji i niszczenia superpozycji stanów pozostałych kubitów. Dlatego też wszystkie algorytmy kwantowe formułowane są w języku obliczeń odwracalnych (a konkretnie za pomocą macierzy unitarnych), a ewentualne efekty nieodwracalne to efekty wynikające z niedoskonałej implementacji, przed którą należy chronić obliczenia za pomocą tzw. protokołów kwantowej korekcji błędów.

Okazuje się, że podobnie jak w obliczeniach klasycznych, dowolną operację kwantową na N kubitach można wykonać, składając ją z względnie prostych operacji elementarnych. Wystarczą do tego operacje jednokubitowe, czyli działające na pojedynczy kubit, za pomocą których można przekształcić dowolną superpozycję stanu kubitu w dowolną inną (wystarczą macierze H i T ze strony 3) oraz jeden typ bramki dwukubitowej, którą najczęściej jest tzw. bramka CNOT (controlled-NOT). Oznaczmy przez $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ stany dwóch kubitów, z których każdy ma dobrze określoną wartość logiczną 0 lub 1. Ogólny stan dwóch kubitów będzie dowolną superpozycją tych stanów. Bramka CNOT zmienia stan drugiego kubitu na przeciwny w sytuacji, gdy pierwszy kubit jest w stanie $|1\rangle$, a pozostawia go bez zmian, jeśli pierwszy kubit znajduje się w stanie $|0\rangle$:

$$\begin{array}{l} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \xrightarrow{\text{CNOT}} \begin{array}{l} |00\rangle \\ |01\rangle \\ |11\rangle \\ |10\rangle \end{array}$$

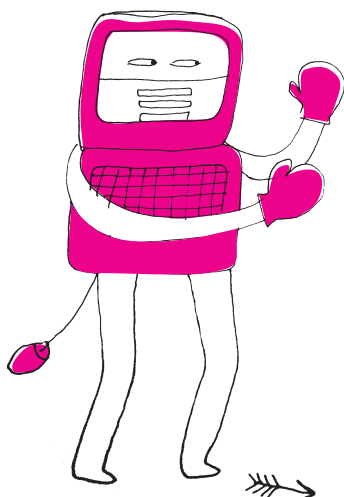
Aby działanie tej bramki było rzeczywiście w pełni kwantowe, musi ona działać w sposób liniowy na dowolne superpozycje stanów wejściowych, dając na wyjściu odpowiednią superpozycję stanów wyjściowych.

Mając już wybraną architekturę obliczeń kwantowych, możemy się skupić na jej fizycznej implementacji. Fizycy próbują budować bramki kwantowe, wykorzystując różne układy fizyczne: jony w pułapkach elektromagnetycznych, fotony poruszające się w wieloramiennych interferometrach optycznych, układy nadprzewodzące, neutralne atomy w sieciach optycznych, kropki kwantowe i wiele



Polak potrafi

W dniach 30–31 sierpnia 2017 roku odbył się (tradycyjnie w Paryżu) międzynarodowy finał 31. Mistrzostw Świata w Grach Matematycznych i Logicznych. W finale biorą udział reprezentacje poszczególnych krajów, wyłonione w drodze krajowych eliminacji. W roku akademickim 2016/17 polskich eliminacji nie zorganizowano, jednak do organizatorów (Francuskiej Federacji Gier Matematycznych) zgłosiły się dwie osoby z Polski z prośbą o indywidualne dopuszczenie do eliminacji. Prośbę spełniono i obie dotarły do finałów w swoich kategoriach wiekowych, kontynuując w ten sposób ciąg wcześniejszych sukcesów polskich uczestników Mistrzostw: Mirosław Zajdel został mistrzem świata w kategorii GP (dorośli niezawodowcy), Robert Ciężabka zajął 7. miejsce w kategorii L2 (studenci). Zadania można znaleźć na naszej stronie.



innych. My skupimy się tutaj na eksperymentach jonowych, gdyż są one z jednej strony najłatwiejsze do zrozumienia, a z drugiej dzięki nim osiąga się największe sukcesy w realizacji bramek kwantowych.

W standardowym eksperymencie tego typu N jonów umieszczonych zostaje w tzw. liniowej elektromagnetycznej pułapce Paula, w której ruch jonów jest praktycznie jednowymiarowy. Siła odpychania kulombowskiego pomiędzy jonami powoduje, że jony znajdują się w odległościach rzędu kilku-kilkudziesięciu μm , co pozwala świecić widzialnym światłem laserowym selektywnie na każdy z jonów osobno. Podstawowym warunkiem użycia danego jonu do obliczeń kwantowych jest istnienie w nim dwóch poziomów energetycznych o długim czasie życia, które mogą pełnić rolę logicznych stanów kubitu $|0\rangle$, $|1\rangle$, a które w dalszym ciągu oznaczymy jako $|g\rangle$, $|e\rangle$, od angielskiego *ground* (podstawowy) i *excited* (wzbudzony). Przykładowo, dla jonu wapnia $^{40}\text{Ca}^+$ będą to stan podstawowy $^2S_{1/2}$ oraz metastabilny stan wzbudzony $^2D_{5/2}$ o czasie życia rzędu 1 s. Wszystkie jony są początkowo przygotowywane w stanie podstawowym. Następnie, świecąc przez odpowiednio dobrany czas światłem laserowym o częstotliwości ω równej częstotliwości przejścia atomowego, można doprowadzić do pochłonięcia przez jon fotonu i tym samym przeprowadzić go do stanu wzbudzonego. Jeśli operację tę zastosujemy z kolei do jonu, który początkowo był już w stanie wzbudzonym, przeprowadzimy go z powrotem do stanu podstawowego (emisja wymuszona). W ten sposób realizujemy operację, która zamienia stany $|g\rangle$ i $|e\rangle$, a tym samym otrzymujemy kwantową wersję bramki NOT. Jeśli natomiast, na jon w stanie $|g\rangle$ będziemy świecić tym samym światłem przez krótszy czas, nie doprowadzimy do pełnego wzbudzenia jonu i znajdzie się on w superpozycji stanów $|g\rangle$, $|e\rangle$. W ten sposób możemy przygotować dowolną superpozycję stanów $|g\rangle$ i $|e\rangle$, a tym samym zrealizować dowolne operacje jednokubitowe. Wiemy, że dla realizacji obliczeń kwantowych potrzebujemy jeszcze bramki dwukubitowej, np. CNOT. To jest już znacznie większe wyzwanie, gdyż musimy wykonać operację, w której ewolucja stanu danego jonu będzie zależała od stanu innego.

Z pomocą przychodzi tu fakt, że jony bardzo silnie oddziałują elektrostatycznie i w związku z tym można je wzbudzić do wspólnych drgań w pułapce. Pułapkę możemy z dobrym przybliżeniem traktować jako potencjał oscylatora harmonicznego o częstotliwości Ω , która jest rzędu setek kHz (dla porównania częstotliwość światła widzialnego jest rzędu 10^{15}Hz). Drganie jonów w pułapce jest, oczywiście, skwantowane i mogą one być wzbudzone do energii będącej całkowitą wielokrotnością $\hbar\Omega$. Rozważmy teraz dwa jony. Wprowadzimy następujące oznaczenie opisujące jednocześnie stany wewnętrzne jonów, jak i ich ruch drgający w pułapce. Przykładowo niech stan $|g\rangle \otimes |g\rangle \otimes |n\rangle$ (dalej będziemy pisać skrótowo $|g\rangle|g\rangle|n\rangle$), odpowiada sytuacji, gdy oba jony są w stanie podstawowym oraz są wzbudzone do ruchu drgającego o energii $n\hbar\Omega$. Rozważmy teraz sytuację, gdy $n = 0$, czyli stan opisujący ruch drgający jonów jest również stanem podstawowym. Jeśli teraz poświecimy na pierwszy z jonów będący w stanie podstawowym $|g\rangle$ impulsem laserowym o częstotliwości $\omega + \Omega$, wzbudzimy go do stanu $|e\rangle$, ale z uwagi na nadwyżkę energii dokonamy jednocześnie wzbudzenia kolektywnego drgań jonów o energii $\hbar\Omega$. Jeśli natomiast atom byłby początkowo w stanie $|e\rangle$, padający impuls światła o tej częstotliwości nie zmieni jego stanu. Tego typu operacja zachowuje kwantową superpozycję stanów – dlatego pod wpływem takiego impulsu stan, w którym pierwszy jon znajdowałby się w dowolnej superpozycji stanów $|g\rangle$ i $|e\rangle$, zostałby przekształcony do

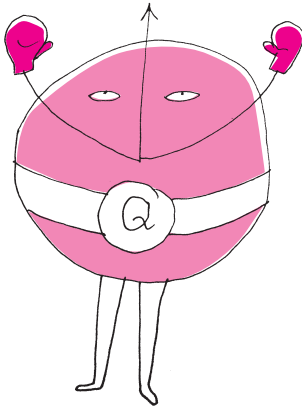
$$(a|g\rangle + b|e\rangle)|g\rangle|0\rangle \rightarrow a|e\rangle|g\rangle|1\rangle + b|e\rangle|g\rangle|0\rangle = |e\rangle|g\rangle(a|1\rangle + b|0\rangle).$$

Zwróćmy uwagę, że w ten sposób „przepisaliśmy” stan wewnętrzny jonu na stan drgań jonów w pułapce. Działając teraz z kolei na drugi jon impulsem o częstotliwości $\omega - \Omega$, będziemy mogli wzbudzić ten jon, ale jedynie w przypadku obecności kwantu energii ruchu drgającego, niezbędnego dla zachowania całkowitej energii w procesie. W efekcie przekształcimy stan do

$$|e\rangle|g\rangle(a|1\rangle + b|0\rangle) \rightarrow a|e\rangle|e\rangle|0\rangle + b|e\rangle|g\rangle|0\rangle = |e\rangle(a|e\rangle + b|g\rangle)|0\rangle.$$

Następnie świecimy impulsem o częstotliwości ω na drugi jon, wykonując na nim operację NOT, i otrzymujemy ostatecznie stan

$$|e\rangle(a|e\rangle + b|g\rangle)|0\rangle \rightarrow |e\rangle(a|g\rangle + b|e\rangle)|0\rangle.$$



W ten sposób przenieśliśmy stan wewnętrzny jonu pierwszego na drugi jon. Pokazuje to, że dzięki pośrednictwu „magistrali” wspólnych drgań jonów możliwe jest wykonywanie operacji wielokubitowych. Nieco bardziej skomplikowany wariant powyższego schematu, którego nie będziemy tu szczegółowo przedstawiać, pozwala w szczególności wykonać operację CNOT, a tym samym dysponować wszystkimi elementami niezbędnymi do zbudowania komputera kwantowego.

Dotychczas w eksperymentach tego typu udało się maksymalnie kontrolować kilkanaście jonów. Dalsze zwiększanie ich liczby prowadzi, niestety, do utraty stabilności układu, jony mogą uciekać z pułapki i pojawiają się dodatkowe efekty psujące kwantową superpozycję. Obecnie trwają prace nad „chipowymi” pułapkami jonowymi, gdzie jony znajdują się w wielu mikropułapkach, pomiędzy którymi mogą być przemieszczane za pomocą sterowania polami elektromagnetycznymi. W ten sposób można przeprowadzić w swoje pobliże jony, na których akurat w danym momencie chcemy wykonać dwukubitową operację, następnie je rozsunąć, zamienić miejscami z innymi jonami znajdującymi się w innej mikropułapce i w ten sposób uniknąć kłopotów związanych z jedną dużą pułapką, która musiałaby kontrolować wszystkie jony równocześnie. Jest to bardzo obiecująca technologia, prace nad nią trwają.

Czy faktycznie komputer kwantowy powstanie w roku 2040? Tego nie wiemy na pewno. Wiemy natomiast, że rozwój technologii związanych z próbami zbudowania komputera kwantowego doprowadził nas do sytuacji, która nie śniła się twórcom teorii kwantowej, a w której jesteśmy w stanie kontrolować i mierzyć pojedyncze układy kwantowe, takie jak atomy i fotony. W eksperymentach z pojedynczymi jonami opisanymi powyżej można w zasadzie zobaczyć pojedynczy jon gołym okiem. Przebyliśmy długą drogę od czasów, gdy eksperymentalnie dostępne nam były jedynie uśrednione wielkości fizyczne zmierzone na bardzo wielu układach kwantowych, a wizje Feynmana wydawały się jedynie spekulacjami geniusza. W ostatnich latach poza ośrodkami akademickimi w rozwijanie technologii związanych z obliczeniami kwantowymi zaczynają angażować się również najwięksi gracze na rynku informatycznym, tacy jak Google, więc może rozwój nabierze tempa ...



Zadania

Redaguje Łukasz BOŻYK

M 1549. Dany jest okrąg ω o średnicy 1 oraz łamana s o końcach należących do tego okręgu, której długość jest mniejsza od 1. Udowodnić, że istnieje średnica okręgu ω , która jest rozłączna z s .

Rozwiązanie na str. 6

M 1550. Dodatnie liczby rzeczywiste a_0, a_1, \dots, a_n są takie, że $\prod_{k=1}^n (a_{k-1} + a_k) = 1$. Udowodnić, że

$$\prod_{k=1}^n (a_{k-1}^2 + ka_k^2) \geq \frac{1}{n+1}.$$

Rozwiązanie na str. 7

M 1551. Wykazać, że każdą dodatnią liczbę całkowitą można zapisać w postaci różnicy dwóch dodatnich liczb całkowitych, które mają tę samą liczbę różnych dzielników pierwszych.

Rozwiązanie na str. 7

Przygotował Michał NAWROCKI

F 941. Gdy czerwone i zielone światło są włączone przez taki sam czas, przed pewnym skrzyżowaniem tworzy się korek. Prędkość samochodów wynosząca normalnie 6 m/s w korku spada do średniej wartości 1,5 m/s (czas włączenia żółtego światła pomijamy). W celu zmniejszenia korka czas włączenia zielonego światła podwojono, nie zmieniając czasu włączenia światła czerwonego. Ile wyniesie średnia prędkość samochodów w korku, jeżeli ich normalna prędkość nie ulegnie zmianie?

Rozwiązanie na str. 10

F 942. Samochód osobowy jedzie równoległe do kolumny ciężarówek poruszających się ze stałą prędkością u w jednakowych odległościach jedna za drugą (odległość przednich zderzaków kolejnych ciężarówek wynosi l). Jeżeli samochód osobowy jedzie z prędkością $v_1 = 36$ km/h, to co $t_1 = 10$ s jest wyprzedzany przez ciężarówkę, a jeżeli jedzie z prędkością $v_2 = 90$ km/h, to on co $t_2 = 10$ s wyprzedza ciężarówkę. Co ile sekund ciężarówki będą mijać samochód osobowy, jeżeli zatrzyma się on na poboczu?

Rozwiązanie na str. 10