1. ERATOSTENES

Wstęp

„Eratostenes, gr. Eratosthenes; ur. 276 p.n.e. w Cyrenie, zm. 194 p.n.e. Grecki matematyk, astronom, filozof, geograf i poeta. Wyznaczył obwód Ziemi oraz oszacował odległość Słońca i Księżyca do Ziemi. Twierdził, że płynąc na zachód od Gibraltaru, można dotrzeć do Indii. Jako pierwszy zaproponował wprowadzenie roku przestępnego, czyli wydłużonego o jeden dodatkowy dzień w kalendarzu. Najważniejsze dzieła Eratostenesa to: *Geographica* – trzytomowe dzieło zawierające podstawy geografii matematycznej i geografii fizycznej (zachowane we fragmentach), *Catasterismi* – dzieło astronomiczne, *Peri komodias* – rozprawa o dawnej komedii. Był również badaczem twórczości Homera – ustalił datę zdobycia Troi na rok 1184 p.n.e., a więc nieodbiegającą od współczesnych szacunków. Podał sposób znajdowania liczb pierwszych – sito Eratostenesa. Przejął po Apolloniosie z Rodos zarządzanie Biblioteką Aleksandryjską".

Najważniejszą i podstawową sprawą w niniejszej pracy będzie algorytm opracowany przez wspomnianego filozofa. Algorytm ten nazwany został **sitem Eratostenesa** ze względu na to, że efekt jego działania przypomina sito, przez którego oczka przelatują liczby pierwsze i w ten sposób sito oddziela je od liczb złożonych. Ponieważ interpretacja tej nazwy może być myląca, będziemy używać nazwy **algorytm Eratostenesa**. Przepis ten pozwala nam znaleźć liczby

pierwsze z pewnego przedziału. Chociaż jest on bardzo znany, to – jak się przekonamy – dzięki niemu zbliżymy się do rozwiązania kilku, o ile nie wszystkich zagadnień związanych z tymi liczbami, wyprowadzając uprzednio pewną wiedzę. Skąd się wziął pomysł, żeby opierając się na tym algorytmie rozwiązywać jakieś zagadki związane z liczbami pierwszymi? Przecież po pierwsze, został on podany dawno, ale to dawno temu, znają i stosują go niemal wszyscy, przede wszystkim w szkole, kiedy to zapoznajemy się z matematyką na poziomie elementarnym oraz gdy uczymy się algorytmów (i gdy usiłujemy złamać ich kod). Co jest w nim takiego ciekawego? Po drugie, to jest tylko algorytm. Czy można zatem w jakiś sposób wyprowadzać z niego twierdzenia i definicje? W wielkim skrócie możemy wyjaśnić to tak: rozpatrzmy przykładowo liczby naturalne z przedziału od 2 do 25; po zastosowaniu tego algorytmu odnajdziemy następujące liczby pierwsze: 2, 3, 5, 7, 11, 13, 17, 19, 23. Następnie wynik ten skonfrontujmy z zagadkami związanymi z liczbami pierwszymi w szczególnych przypadkach. Ile jest liczb pierwszych nie większych niż 25? Dokładnie 9 liczb. Czy istnieją takie liczby pierwsze p, że $2 \cdot p + 1$ też jest liczbą pierwszą? Tak, są to: 2, 3, 5, 11. Czy istnieją takie liczby pierwsze p, że $p + 2$ też jest liczbą pierwszą? Tak, są to: 3 i 5, 5 i 7, 11 i 13, 17 i 19. Czy dla parzystej liczby 10 istnieją dwie takie liczby pierwsze p i q, że $p + q = 10$? Tak, są to pary 5 i 5 oraz 3 i 7. Czy to samo możemy powiedzieć o jakiejś innej liczbie parzystej, np. 12, 14, 16? Owszem, możemy. Możemy spytać też inaczej: jakie liczby parzyste uzyskamy z dostępnych liczb pierwszych? Odpowiedź na to pytanie, choć nie jest tak oczywista, wkrótce stanie się zdumiewająco prosta i jasna jak słońce. A zatem możemy odpowiedzieć na te pytania, wskazując, które to liczby, lub określając, ile ich jest, analizując to, co otrzymaliśmy po wykonaniu tegoż algorytmu. Ponieważ N może być dowolną liczbą naturalną, więc nasze pytania możemy stawiać dla każdej takiej liczby. Natomiast przy N dążącym do nieskończoności powinniśmy otrzymać cały zbiór liczb pierwszych i wszystkie odpowiedzi na dręczące nas pytania z nimi związane. Czy uda się to zrobić? Przekonajmy się, zaczynając od podstawowego

twierdzenia, drobnej uwagi na temat samego algorytmu, od sformułowania jego definicji oraz kilku modyfikacji.

Podstawa

Definicję tego algorytmu moglibyśmy zapożyczyć z dowolnego źródła i w każdym z nich z pewnością znajdziemy to, co jest dla nas interesujące, tzn. przepis, jak znaleźć liczby pierwsze. Ponieważ ja znalazłem coś więcej niż tylko przepis, coś, co doprowadzi nas do ciekawych wniosków, więc chcąc się tym podzielić, wybrałem tekst, którego autorem jest **Wacław Sierpiński** (Sierpiński 1987). Tekst dotyczy algorytmu podanego przez Eratostenesa, a my poddamy go drobnej analizie.

Twierdzenie 1 o dzielniku liczby złożonej
Każda liczba złożona z ma dzielnik pierwszy $p \leq \sqrt{z}$.

„Z twierdzenia tego wynika, że żeby przekonać się, czy liczba naturalna $z > 1$ jest liczbą pierwszą, wystarczy dzielić ją przez liczby naturalne > 1 oraz $\leq \sqrt{z}$. Wynika stąd, że dla otrzymania wszystkich liczb pierwszych zawartych w ciągu 2, 3, 4, ..., m, gdzie m jest daną liczbą naturalną > 1, wystarczy z tego ciągu usunąć wszystkie wielokrotności $k \cdot p$ liczb pierwszych $p \leq \sqrt{m}$, gdzie $k > 1$. Więc na przykład, aby otrzymać wszystkie liczby pierwsze ≤ 100, wystarczy usunąć z ciągu 2, 3, 4, ..., 100 wszystkie liczby większe niż 2, 3, 5, 7 i podzielne przez jedną co najmniej z tych czterech liczb. Łatwy sposób znajdywania kolejnych liczb pierwszych podany został przez matematyka starożytnej Grecji, Eratostenesa. Weźmy pod uwagę ciąg 2, 3, 4, ... Ponieważ 2 jest najmniejszą liczbą pierwszą p_1, więc usuwamy z naszego ciągu wszystkie liczby $> p_1$ i podzielne przez p_1. Pierwszą z pozostałych $> p_1$ liczb jest liczba $3 = p_2$. Usuwamy teraz z naszego

ciągu wszystkie liczby $> p_2$ i podzielne przez p_2. Pierwszą z pozostałych $> p_2$ liczb jest liczba $5 = p_3$. Usuwamy teraz z naszego ciągu wszystkie liczby $> p_3$ i podzielne przez p_3. Przypuśćmy, że powtórzywszy nasze postępowanie *i* razy, otrzymaliśmy *i*-tą liczbę pierwszą p_i. Usuwamy wówczas z naszego ciągu wszystkie liczby $> p_i$ i podzielne przez p_i. Najmniejszą z nieusuniętych dotąd liczb większych od p_i będzie $i + 1$ liczba pierwsza p_{i+1}. Jeżeli naszym ciągiem jest ciąg 2, 3, 4, ..., *N*, to postępowanie nasze możemy zakończyć, otrzymawszy największą liczbę pierwszą $p_j \leq \sqrt{N}$ i usunąwszy jej wielokrotności. Wszystkie większe od niej pozostałe liczby będą pierwsze".

Pierwszą rzecz, jaką można zauważyć w tym algorytmie, wynosimy z faktu, że wyrażenie $p \leq \sqrt{N}$ jest równoważne wyrażeniu $p^2 \leq N$, gdyż *p* jest dodatnie, więc i *N* musi takie być. A stąd wnioskujemy indukcyjnie, że w szczególnym przypadku, gdy nasze $N = 4 = 2^2$, to żeby znaleźć wszystkie liczby pierwsze od 2 do 4, wystarczy usunąć wszystkie wielokrotności liczby 2, tzn. liczbę $2 \cdot 2 = 4$, czy też po prostu 2^2. Pozostałe liczby będą pierwsze. Gdy $N = 9 = 3^2$, to żeby znaleźć wszystkie liczby pierwsze od 2 do 9, wystarczy powtórzyć postępowanie z liczbą 2, tzn. usunąć 2^2, po czym pozostałe wielokrotności liczby 2. Następnie usuwamy wszystkie pozostałe wielokrotności liczby 3, zaczynając od liczby $3 \cdot 3 = 9$, tj. po prostu 3^2, gdyż nie ma już mniejszej wielokrotności liczby 3, liczba $3 \cdot 2 = 6$ została bowiem już usunięta. I ogólnie, gdy liczba *N* jest kwadratem *i*-tej z kolei liczby pierwszej p_i^2, to żeby znaleźć wszystkie liczby pierwsze od 2 do p_i^2, wystarczy usunąć 2^2 oraz pozostałe wielokrotności liczby 2. Następnie 3^2 oraz wszystkie pozostałe wielokrotności liczby 3. Gdy dojdziemy do *i*-tej z kolei liczby pierwszej p_i, to pierwszą wielokrotnością tej liczby nie jest liczba $2 \cdot p_i$, ani też liczby $3 \cdot p_i$, $5 \cdot p_i$ itd., gdyż te wielokrotności zostały już usunięte przy okazji usuwania wielokrotności liczb pierwszych mniejszych od p_i. Pierwszą nieusuniętą wielokrotnością liczby p_i jest liczba p_i^2 i jest to

ostatnia liczba złożona, jaką trzeba usunąć. Gdy N jest liczbą złożoną niebędącą kwadratem liczby pierwszej, to w myśl **twierdzenia 1** postępowanie kończymy, gdy dojdziemy do takiej liczby pierwszej p, że $p^2 \leq N$, więc gdy dotrzemy do j-tej z kolei liczby pierwszej p_j takiej, że $p_j^2 \leq N$, a $p_{j+1}^2 > N$. Wówczas usuwamy liczbę p_j^2 i wszystkie pozostałe jej wielokrotności, o ile istnieją. Ponieważ usunęliśmy wszystkie wielokrotności liczb pierwszych p, za każdym razem zaczynając od p^2, więc pozostałe zawarte od 2 do N muszą być liczbami pierwszymi. Przydałaby się też jakaś wiedza, jak najłatwiej usunąć takie wielokrotności. Sprawa wydaje się łatwa, bowiem wielokrotności $> p_1$ to liczby 4, 6, 8, ..., które występują jako co druga w ciągu 2, 3, 4, ... **[1]**, licząc od liczby 2, z których pierwsza jest kwadratem pierwszej liczby pierwszej. Dalej, wielokrotności $> p_2$ to liczby 6, 9, 12, ..., które występują jako co trzecia w ciągu **[1]**, licząc od liczby 3 i z których druga jest kwadratem drugiej liczby pierwszej, a pierwsza z nich, a jest to liczba 6, jest wielokrotnością poprzedniej liczby pierwszej. Wobec czego usuwamy liczbę 3^2 i od niej co trzecią, poprzestając na takiej wielokrotności liczby p_1, że $p_1 \cdot k \leq N$. Następne wielokrotności $> p_3$ to liczby $10,\ 15,\ 20, \ldots$, które występują jako co piąta w ciągu **[1]**, licząc od liczby 5 i z których czwarta jest kwadratem trzeciej liczby pierwszej, a poprzednie, tj. liczby 10, 20, 30, są również wielokrotnościami poprzednich liczb pierwszych. I dlatego usuwamy liczbę 5^2 i od niej co piątą, poprzestając na takiej wielokrotności k liczby p_2, że $p_2 \cdot k \leq N$. I tak dalej... Postępowanie to kończymy, gdy dojdziemy do i-tej z kolei liczby pierwszej p_i takiej, że $p_i \leq N$. W istocie, jeśli warunek ten jest spełniony, to począwszy od liczby p_i usuwamy co p_i-tą liczbę, zaczynając od jej kwadratu, tzn. usuwamy liczby: $p_i \cdot p_i$, $p_i \cdot p_i + p_i$ itd. i poprzestając na takiej wielokrotności $k \cdot p_i$ liczby p_i, że $p_i \cdot k \leq N$. Liczby postaci $p_1 \cdot p_i$, $p_2 \cdot p_i$, ..., $p_{i-1} \cdot p_i$ zostały już usunięte. W ostatnim kroku należy jeszcze tylko sprawdzić, czy faktycznie jest tak, że $p_{i+1} > N$. Jeśli tak, to usunęliśmy wszystkie wielokrotności większe od liczb pierwszych i nie

większe niż N, z czego wynika, że pozostałe to liczby pierwsze. Taka jest zasada działania algorytmu Eratostenesa.

Przemyślenia te nie wnoszą niczego nowego do naszej wiedzy na temat liczb pierwszych. Algorytm jest trochę zmodyfikowany i działa nieco szybciej. Z pewnością nie jestem pierwszą osobą, która zauważyła, że usuwanie liczb złożonych można zacząć od podniesienia kolejno znalezionej liczby pierwszej do kwadratu. Jednakże przykład ten uzmysławia nam, że coś jest na rzeczy. Pytanie, jakie należy postawić w tym momencie, brzmi: czy to już wszystko, co można zauważyć, analizując treść, przebieg czy efekt działania tego algorytmu? Sprawdźmy kolejne spostrzeżenia.

Co i gdzie?

W naszych rozważaniach dotyczących tego, od której liczby należałoby zacząć usuwanie, wskazaliśmy, w jaki sposób usunąć wielokrotności kolejnych liczb pierwszych i gdzie występują te liczby, wobec czego wydaje się logiczne, by usunąć je właśnie stamtąd, tzn. z tego ciągu, w którym występują. Czy aby na pewno? Zauważmy, że w podanym algorytmie cały czas przewija się stwierdzenie „nasz ciąg". Mowa tu o ciągu liczb 2, 3, 4, …, to on jest „naszym ciągiem". Następnie jest powiedziane, że usuwamy z „naszego ciągu" wszystkie liczby $> p_1$ i podzielne przez p_1. Załóżmy, że $N = 25$, wtedy „nasz ciąg" przyjmie postać: 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25 **[2]**. Usuńmy z niego wielokrotności liczby $p_1 = 2$ i od niej większe. Najłatwiej jest to zrobić, usuwając co drugą liczbę licząc od liczby 2. Będą to liczby: 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24 **[3]**. Ponieważ jest polecenie, żeby usunąć te liczby z „naszego ciągu", więc tak zróbmy. Otrzymamy wtedy następujący ciąg: 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25 **[4]**. Po usunięciu liczb **[3]** z „naszego ciągu", otrzymamy właśnie ciąg **[4]**, a nie żaden inny. Następnym krokiem jest usunięcie z „naszego ciągu" wszystkich wielokrotności kolejnej napotkanej liczby, tzn. pierwszej napotkanej, która jest drugą z kolei liczbą

pierwszą $p_2 = 3$. Przypomnijmy, że „nasz ciąg" to **[2]** i faktycznie jest tak, że w tym ciągu pierwszą napotkaną liczbą jest druga z kolei liczba pierwsza $p_2 = 3$. I znowu jest kolejne polecenie, żeby usunąć liczby z ciągu **[2]**, który wg założenia jest „naszym ciągiem". Usuńmy zatem z niego wielokrotności liczby 3 i od niej większe. Usuwając co trzecią liczbę, począwszy od liczby 3, tzn. liczby: 6, 9, 12, 15, 18, 21, 24 **[5]**, otrzymamy następujący ciąg: 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25 **[6]**. Po usunięciu liczb **[5]** z „naszego ciągu", otrzymamy ciąg **[6]**. Dalej mamy powiedziane, że pierwszą napotkaną liczbą > 3 jest kolejna liczba pierwsza równa 5. W „naszym ciągu" nic się nie zmieniło, a w nim kolejna liczba to 4. W powstałym ciągu **[6]** pierwszą nieusuniętą liczbą jest również 4. Doszliśmy zatem do sprzeczności. Mamy jeszcze ciąg **[4]**, a w nim pierwszą napotkaną liczbą > 3 jest faktycznie kolejna liczba pierwsza równa 5. Jednak z pewnością nie chodzi o ten ciąg, gdyż liczba 9, która jest złożona, nie została usunięta. Dalsze postępowanie traci sens, gdyż już teraz widzimy, że nie doprowadzi nas ono do pożądanego wyniku.

Błąd ten, choć jest do zlokalizowania i łatwy do usunięcia, jest całkiem sensowny, o ile zdołamy sprecyzować nasze postępowanie. Gdzie zatem został on popełniony i na czym polega? Bez większego namysłu stwierdzamy, że błąd polega na tym, iż nie powinniśmy usuwać żadnych liczb, tylko za każdym razem zaznaczać (w jakikolwiek sposób) wielokrotności liczb pierwszych i od nich większe, wtedy faktycznie otrzymamy zbiór liczb pierwszych $\leq N$. Gdy zaczynamy usuwać wielokrotności liczb pierwszych i od nich większe, dochodzi do pewnych nieścisłości oraz oprócz jednego rozpatrywanego ciągu za każdym razem, kiedy usuwamy liczby, otrzymujemy jakieś dodatkowe inne ciągi.

Doszliśmy zatem do takiego wniosku, że istotne jest, **co robimy i na czym to robimy**. W tym przypadku ważne jest to, czy zaznaczamy, czy też faktycznie usuwamy liczby z ciągu oraz na jakim ciągu pracujemy. I stąd właśnie zrodził się pomysł. Oczywiście z samego algorytmu *ergo* z wykonywanych czynności nie za dużo można wynieść. Można natomiast przyjrzeć się uważnie jego treści, efektowi

końcowemu lub poszczególnym etapom jego działania. Mając takie elementy, jak:

1. twierdzenie,
2. definicję/ treść,
3. działanie,
4. efekt,

z których każdy kolejny wynika z poprzedniego, tzn. z twierdzenia wynika definicja algorytmu, z definicji – jego działanie, z działania – efekt w postaci liczb pierwszych z pewnego przedziału, zastanowimy się nad następującymi zagadnieniami:

1. Jak ma się treść do efektu?
2. Jak zmienić treść, nie zmieniając przy tym efektu?
3. Jaki efekt otrzymamy, jeśli zmodyfikujemy treść?

Postawione pytania mają nas doprowadzić do rozwiązania jakiegoś zagadnienia, np. związanego z hipotezą liczb pierwszych bliźniaczych. Ponieważ nie widać bezpośredniego związku tych zadań z algorytmem, a właściwie jedyne, co widać, to fakt, że sprawa dotyczy liczb pierwszych, postawmy więc sobie cel pośredni, jakim będzie szczegółowe zrozumienie działania algorytmu. Pozwoli nam to odpowiedzieć na pytanie 1, następnie niejako udostępni nam odpowiedź na pytanie 2, po czym przejdziemy do szukania odpowiedzi na pytanie 3.

Algorytmy

W pierwszej kolejności, mając na uwadze rozróżnienie między **usuwaniem** a **zaznaczaniem** liczb oraz ciąg, na jakim pracujemy, podamy jednoznaczną definicję postępowania, przetłumaczoną na język naturalny i język programowania cpp. Oznaczmy ją **Alg. E1 v2 –** co *p*-ta, co należy rozumieć następująco: **Alg.** – algorytm Eratostenesa, **E1** – ciąg liczb, **v** – wartości, **2** – wersja 2, co *p*-ta – zaznaczamy co *p*-tą liczbę.

Alg. E1 v2 – co *p*-ta

Żeby z ciągu liczb 2, 3, 4, ..., N otrzymać wszystkie liczby pierwsze, wystarczy zaznaczyć następujące liczby:
liczbę $2 \cdot 2$ oraz co 2-gą od niej, kończąc na największej takiej liczbie i, że $i \leq N$,
liczbę $3 \cdot 2$ oraz co 3-cią od niej, kończąc na największej takiej liczbie i, że $i \leq N$,
liczbę $5 \cdot 2$ oraz co 5-tą od niej, kończąc na największej takiej liczbie i, że $i \leq N$,
...,
liczbę $p \cdot 2$ oraz co p-tą od niej, kończąc na największej takiej liczbie i, że $i \leq N$.
Postępowanie kończymy na największej takiej liczbie pierwszej q, że $q^2 \leq N$.
Wszystkie niezaznaczone liczby są liczbami pierwszymi.

c++: **Alg. E1 v2** – co *p*-ta

```
#include<iostream>
#include<cstdlib>
using namespace std;
int main()
{
   int N; int *tab;
   cout<<"podaj N: "; cin>>N;
   tab = new int[N+1];
   tab[0] = 0; tab[1] = 0;
   for(int i=2; i<=N; i++) tab[i] = 1;
   for(int i=2; i*i<=N; i++)
   {
      if(tab[i]) for(int j = 2*i ; j<=N; j+=i) tab[j]=0;
   }
   for(int i=2; i<=N; i++) if(tab[i]) cout<<i<<endl;
   delete [] tab; system("pause"); return 0;
}
```

Pasek zaznaczony na szaro to region krytyczny algorytmu, sedno sprawy. Zakładając, że mamy zdeklarowany przykładowy ciąg liczb od 2 do 25, prześledźmy działania tego obszaru, ujmując je w treść (tzn. napiszemy, co robimy, ale tego nie zrobimy), a następnie zwizualizujemy to postępowanie:

1. dany jest ciąg liczb (tabela 1),
2. bierzemy liczbę 2 i sprawdzamy, czy $2^2 \leq 25$,
3. jest, więc sprawdzamy, czy 2 jest liczbą pierwszą,
4. jest, więc zaznaczamy liczby: $2 \cdot 2,\ 2 \cdot 2 + 2,\ 2 \cdot 2 + 2 + 2,$ …, tj. co drugą liczbę aż do takiej wielokrotności $2 \cdot k$ liczby 2, że $2 \cdot k \leq 25$, tzn. do liczby 24 (tabela 2),
5. dodajemy 1 do liczby 2 i sprawdzamy, czy $3^2 \leq 25$,
6. jest, więc sprawdzamy, czy 3 jest liczbą pierwszą,
7. jest, więc zaznaczamy liczby: $2 \cdot 3,\ 2 \cdot 3 + 3,\ 2 \cdot 3 + 3 + 3,$ …, a są to liczby co trzecia aż do takiej wielokrotności $3 \cdot k$ liczby 3, że $3 \cdot k \leq 25$, tzn. do liczby 24 (tabela 3),
8. dodajemy 1 do liczby 3 i sprawdzamy, czy $4^2 \leq 25$,
9. jest, więc sprawdzamy, czy 4 jest liczbą pierwszą,
10. nie jest, więc dodajemy 1 do liczby 4 i sprawdzamy, czy $5^2 \leq 25$,
11. jest, więc sprawdzamy, czy 5 jest liczbą pierwszą,
12. jest, więc zaznaczamy liczby: $2 \cdot 5,\ 2 \cdot 5 + 5,\ 2 \cdot 5 + 5 + 5,$ …, jest to co piąta liczba aż do takiej wielokrotności $5 \cdot k$ liczby 5, że $5 \cdot k \leq 25$, tzn. do liczby 25 (tabela 4),
13. dodajemy 1 do liczby 5 i sprawdzamy, czy $6^2 \leq 25$,
14. nie jest, więc kończymy algorytm.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 1

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 2

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 3

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 4

Efektem naszego działania jest zbiór liczb pierwszych ≤ 25. Oznacza to, że znaleźliśmy wszystkie liczby pierwsze z ciągu liczb od 2 do 25. A jak się ma do tego treść algorytmu? Otóż mówi nam, że jeśli chcemy znaleźć wszystkie liczby pierwsze, to musimy zaznaczyć jakieś inne liczby, które są wielokrotnościami kilku początkowych liczb pierwszych, tzn. w tym przypadku znaleźliśmy liczbę 2 i wszystkie jej wielokrotności nie większe niż 25, a więc łącznie liczby: 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, następnie liczbę 3 i wszystkie jej wielokrotności nie większe niż 25, tj. łącznie liczby: 3, 6, 9, 12, 15, 18, 21, 24 oraz liczbę 5 i wszystkie jej wielokrotności nie większe niż 25, łącznie liczby: 5, 10, 15, 20, 25. Innymi słowy, żeby znaleźć wszystkie liczby pierwsze od 2 do 25, musimy znaleźć i zaznaczyć wszystkie takie liczby z tego przedziału, które nie są liczbami pierwszymi, po czym stwierdzamy, że pozostałe są tymi, których szukamy. Wynika stąd, że *de facto* znaleźliśmy tylko liczby pierwsze od 2 do $\sqrt{25}$ oraz liczby złożone ≤ 25. I tak ma się właśnie treść do efektu, tzn. szukamy, znajdujemy i zaznaczamy prawie zupełnie coś innego, po czym stwierdzamy, że to, czego szukaliśmy jest tym, czego nie znaleźliśmy. W istocie, nie ma w tym nic dziwnego. Natomiast fakt, że twierdzimy, iż znaleźliśmy liczby pierwsze z tego przedziału wynika stąd, że zbiór liczb naturalnych N większych od liczby jeden można uzyskać, sumując zbiór liczb złożonych Z ze zbiorem liczb pierwszych P. Jeżeli mając taki podzbiór liczb naturalnych w postaci ciągu 2, 3, 4, … lub w postaci zbioru $N\backslash\{1\} = E$, uda nam się znaleźć skończoną liczbę początkowych liczb lub nawet wszystkie liczby złożone, to w myśl algorytmu Eratostenesa wszystkie pozostałe (odpowiednio) nie większe od

pewnej liczby lub nawet wszystkie pozostałe będą pierwsze. Zatem jeśli ze zbioru E usuniemy lub zaznaczymy zbiór Z (w dowolny sposób), to otrzymamy zbiór P. W skrócie: $P = E \backslash Z$. Jest to twierdzenie wynikające natychmiast z definicji tych liczb. Mając to na uwadze oraz rozumiejąc działanie tego algorytmu, możemy przejść do manipulowania definicją algorytmu, ale tak, by nie zmieniać efektu jego działania, nie wnikając przy tym w szczegóły.

Spostrzeżenie dotyczące faktu, od której liczby zacząć wykreślanie, zapiszmy w kolejnym algorytmie:

Alg. E1 v3 – od p^2

Żeby z ciągu liczb 2, 3, 4, … , N otrzymać wszystkie liczby pierwsze, wystarczy zaznaczyć następujące liczby:
liczbę $2 \cdot 2$ oraz co 2-gą od niej, kończąc na największej takiej liczbie i, że $i \leq N$,
liczbę $3 \cdot 3$ oraz co 3-cią od niej, kończąc na największej takiej liczbie i, że $i \leq N$,
liczbę $5 \cdot 5$ oraz co 5-tą od niej, kończąc na największej takiej liczbie i, że $i \leq N$,
…,
liczbę $p \cdot p$ oraz co p-tą od niej, kończąc na największej takiej liczbie i, że $i \leq N$.
Postępowanie kończymy na największej takiej liczbie pierwszej q, że $q^2 \leq N$.
Wszystkie niezaznaczone liczby są liczbami pierwszymi.

W tym algorytmie pierwszą zaznaczaną wielokrotnością kolejnych liczb pierwszych p są ich kwadraty, a w **Alg. E1 v2** są to liczby postaci $p \cdot 2$. Działają one trochę inaczej, ale rezultat jest taki sam.

Można spotkać się jeszcze z jedną definicją tego algorytmu, która okaże się niezwykle przydatna w naszych rozważaniach, dlatego też ją przytoczymy oraz uzasadnimy, że wynik działania tegoż algorytmu jest identyczny jak w poprzednio przedstawionych.

Alg. E1 v0 – co n-ta
Żeby z ciągu liczb 2, 3, 4, …, N otrzymać wszystkie liczby pierwsze, wystarczy zaznaczyć następujące liczby: liczbę $2 \cdot 2$ oraz co 2-gą od niej, kończąc na największej takiej liczbie i, że $i \leq N$, liczbę $3 \cdot 2$ oraz co 3-cią od niej, kończąc na największej takiej liczbie i, że $i \leq N$, liczbę $4 \cdot 2$ oraz co 4-tą od niej, kończąc na największej takiej liczbie i, że $i \leq N$, …, liczbę $n \cdot 2$ oraz co n-tą od niej, kończąc na największej takiej liczbie i, że $i \leq N$. Postępowanie kończymy na największej takiej liczbie j, że $j^2 \leq N$. Wszystkie niezaznaczone liczby są liczbami pierwszymi.

W **Alg. E1 v0** oprócz wielokrotności liczb pierwszych $p \cdot m$ zakreślamy również wielokrotności liczb złożonych $z \cdot m$ przy naturalnym $m > 1$. Po pierwsze, zakreślamy **tylko liczby złożone**, bo każda liczba przez nas zakreślona jest podzielna przez m, a przecież $m > 1$. A zatem pomijając te liczby, otrzymamy **Alg. E1 v2**, skąd wnosimy, że efekty tych działań są takie same. Należy dodać, że zarówno w jednym, jak i w drugim algorytmie zaznaczamy **wszystkie** liczby złożone, bo skoro algorytm wyznacza wszystkie liczby pierwsze nie większe niż N, to nie mogliśmy pominąć ani jednej liczby złożonej. W przeciwnym razie żaden z algorytmów nie byłby poprawny i wyznaczałby np. wszystkie liczby pierwsze i jeszcze kilka złożonych lub wyznaczałby prawie wszystkie liczby pierwsze. Algorytm ten został oznaczony jako **wersja 0**, gdyż w zasadzie powinien on być przedstawiony jako pierwszy, a dopiero potem można wywnioskować, że nie ma potrzeby zaznaczania wielokrotności liczb złożonych $z \cdot m$, gdyż zostały one już wcześniej zaznaczone, przy okazji zaznaczania wielokrotności liczb pierwszych $p < z$. Przebieg tego algorytmu będzie wyglądał następująco:

1. dany jest ciąg liczb (tabela 1),
2. bierzemy liczbę 2 i sprawdzamy, czy $2^2 \leq 25$,
3. jest, więc zaznaczamy co drugą liczbę: $2 \cdot 2$, $2 \cdot 2 + 2$, $2 \cdot 2 + 2 + 2$, ..., aż do takiej wielokrotności $2 \cdot k$ liczby 2, że $2 \cdot k \leq 25$, tzn. do liczby 24 (tabela 2),
4. dodajemy 1 do liczby 2 i sprawdzamy, czy $3^2 \leq 25$,
5. jest, więc zaznaczamy co trzecią liczbę: $2 \cdot 3$, $2 \cdot 3 + 3$, $2 \cdot 3 + 3 + 3$, ..., aż do takiej wielokrotności $3 \cdot k$ liczby 3, że $3 \cdot k \leq 25$, tzn. do liczby 24 (tabela 3),
6. dodajemy 1 do liczby 3 i sprawdzamy, czy $4^2 \leq 25$,
7. jest, więc zaznaczamy co czwartą liczbę: $2 \cdot 4$, $2 \cdot 4 + 4$, $2 \cdot 4 + 4 + 4$, ..., aż do takiej wielokrotności $4 \cdot k$ liczby 4, że $4 \cdot k \leq 25$, tzn. do liczby 24,
8. dodajemy 1 do liczby 4 i sprawdzamy, czy $5^2 \leq 25$,
9. jest, więc zaznaczamy co piątą liczbę: $2 \cdot 5$, $2 \cdot 5 + 5$, $2 \cdot 5 + 5 + 5$, ..., aż do takiej wielokrotności $5 \cdot k$ liczby 5, że $5 \cdot k \leq 25$, tzn. do liczby 25 (tabela 4),
10. dodajemy 1 do liczby 5 i sprawdzamy, czy $6^2 \leq 25$,
11. nie jest, więc kończymy algorytm.

Działanie tego algorytmu wygląda podobnie i różni się jedynie tym, że nie sprawdzamy, czy liczba jest pierwsza oraz tym, że zaznaczamy również wielokrotności kolejnych liczb złożonych.

Możemy przekształcić **Alg. E1 v0**, dopisując do jego definicji, żeby podnosić do kwadratu i zaznaczać również liczby złożone, nie zmieniając przy tym końcowego wyniku. Otrzymamy kolejny algorytm:

Alg. E1 v1 – od n^2

Żeby z ciągu liczb 2, 3, 4, ..., N otrzymać wszystkie liczby pierwsze, wystarczy zaznaczyć następujące liczby:
liczbę 2^2 oraz co 2-gą od niej, kończąc na największej takiej liczbie i, że $i \leq N$,
liczbę 3^2 oraz co 3-cią od niej, kończąc na największej takiej liczbie i,

że $i \leq N$,
liczbę 4^2 oraz co 4-tą od niej, kończąc na największej takiej liczbie *i*, że $i \leq N$,
…,
liczbę n^2 oraz co *n*-tą od niej, kończąc na największej takiej liczbie *i*, że $i \leq N$.
Postępowanie kończymy na największej takiej liczbie *j*, że $j^2 \leq N$.
Wszystkie niezaznaczone liczby są liczbami pierwszymi.

Pytania

Zauważmy, że subtelne zmiany wprowadzane w definicji, takie jak zmiana liczby, od której zaczynamy zakreślać, czy zakreślanie wielokrotności liczb złożonych, nie zmieniają efektu działania algorytmu. Jedynie uświadamiają, że sprawa jest ciekawa i warta zgłębienia. Ostatnie pytanie, jakie nam zostało, to: **jaki efekt otrzymamy, jeśli zmodyfikujemy treść?** Odpowiedź na to pytanie będzie najtrudniejsza ze względu na wiele różnych możliwości modyfikowania algorytmu. Pamiętając jednak, jaki jest nasz cel, możemy to pytanie sformułować bardziej szczegółowo, otrzymując następujące:

1. Co się stanie, kiedy faktycznie będziemy usuwać liczby, a nie tylko je zakreślać?

2. Co otrzymamy, jak będziemy zaznaczali wszystkie wielokrotności kolejnych liczb pierwszych, tzn. liczby: 2, 4, 6, 8, …, 3, 6, 9, 12, …, 5, 10, 15, 20, … itd., ale do pewnej liczby naturalnej.

Powracając do przytoczonego tekstu, możemy postawić jeszcze kilka pytań. Przypomnijmy: „Weźmy pod uwagę ciąg 2, 3, 4, … Jeżeli naszym ciągiem jest ciąg 2, 3, 4, …, *N*, to postępowanie nasze możemy zakończyć … ”.

3. Co, jeśli nie zadeklarujemy żadnego ograniczenia i *N* będzie nieokreślone? Czy będziemy wykonywali algorytm Erato-

stenesa w nieskończoność, czy też można go w jakiś inny sposób zakończyć?

4. Jaki będzie tego skutek, jeżeli zdeklarowany ciąg zastąpimy innym ciągiem?

Odpowiedzi na te konkretne pytania ujmiemy w kolejnych rozdziałach i będą one stanowić kontynuację **analizy jakościowej** omawianego algorytmu, tzn. co zrobić, by znaleźć liczby pierwsze. Natomiast poszukiwania odpowiedzi na poniższe pytania przedstawimy jako **analizę ilościową**, tzn. jak policzyć liczby, które znaleźliśmy, odpowiadając przy tym na następujące pytania. „Ponieważ 2 jest najmniejszą liczbą pierwszą p_1, więc usuwamy z naszego ciągu wszystkie liczby $> p_1 i$ i podzielne przez p_1…". Tu i wszędzie tam, gdzie znajdujemy kolejne liczby pierwsze i usuwamy czy też zaznaczamy wszystkie jej wielokrotności od niej większe, należy spytać:

5. Ile liczb zaznaczamy, postępując wg algorytmu?

A następnie należałoby zbadać takie obliczenia.

Dalej mamy tak: „Przypuśćmy, że powtórzywszy nasze postępowanie i razy otrzymaliśmy i-tą liczbę pierwszą p_i". Co oznacza, że znaleźliśmy i liczb pierwszych. Po czym jest napisane, że: „Wszystkie większe od niej pozostałe liczby będą pierwsze".

Tzn. jest tak, że o ile p_i jest największą liczbą pierwszą, jaką udało nam się znaleźć, co implikuje, że $p_{i+1}^2 > N$, to wszystkie niezaznaczone liczby od p_i do N są pierwsze.

6. Ile jest liczb, których nie zaznaczamy?

Oczywiście znając odpowiedź na **pytanie 5**, można wywnioskować, jaka jest odpowiedź na **pytanie 6**, jednakże przekonamy się, że obydwa pytania i szukanie na nie odpowiedzi są istotne. Jeśli uda nam się obliczyć, ile liczb zaznaczamy, to czy można stąd wywnioskować, ile zostało?

7. Co możemy powiedzieć o pozostałych liczbach, które nie zostały zaznaczone?

Oczywiście odpowiedzi nie są tak ważne, jak wnioski z nich płynące oraz to, do czego nam się one przydadzą. Niemniej jednak

wszystkie odpowiedzi na te oraz inne pytania postaramy się sukcesywnie opracować w kolejnych rozdziałach, powracając co jakiś czas do przedstawionych modyfikacji algorytmu Eratostenesa oraz wyprowadzając kolejne.

Argumentacja

Obecnie przepis podany przez Eratostenesa wykonywany jest głównie przez komputer. Wcześniej, gdy nie było tej możliwości, algorytm ten był wykonywany klasycznie, tzn. kartka papieru, ołówek i zakreślano liczby wg przepisu. Zazwyczaj żeby tego dokonać, rozpisywano liczby w kolumnach i to przeważnie 10 kolumn po 10 wierszy, ze względu na ograniczoną powierzchnię kartki. Niezwykle trudno byłoby rozpisać liczby np. w 1000 kolumn i 1000 wierszy, a następnie wykonać na tak rozpisanych liczbach algorytm. Byłaby to bardzo długa i żmudna robota, nie wspominając już o tym, że analiza relacji między pozostałymi liczbami pierwszymi byłaby – jakkolwiek przydatna i zapewne cenna – z pewnością niekompletna. Tym bardziej relacji tych nie widać, gdy liczby naturalne > 1 rozpisywane są liniowo:

2	3	4	5	6	7	8	9	10	11	12	13	14	15	...

Tabela 5

Postępując wg algorytmu, znajdujemy liczby 2 i 3 oraz zakreślamy wielokrotności tych liczb od nich większe; otrzymujemy wówczas taki ciąg:

2	3	4	5	6	7	8	9	10	11	12	13	14	15	...

Tabela 6

Znaleźliśmy dwie liczby pierwsze 2 i 3 oraz ich wielokrotności, łącznie są to liczby 2, 4, 6, 8, 10, 12, 14, … oraz 3, 6, 9, 12, 15, … , a o pozostałych wiemy tyle tylko, ile jesteśmy w stanie odczytać, tzn. tyle, na ile

nam ograniczenie kartki ewentualnie powierzchnia monitora pozwoli. Jest to powód, dla którego warto się zastanowić, jak inaczej można rozpisać liczby.

Lepiej sprawa się przedstawia, gdy liczby te rozpiszemy w kolumnach, a pytanie, jakie się nasuwa, to ile tych kolumn powinno być, by móc poddać analizie pozostałe liczby? W pierwszym kroku znajdujemy liczbę 2 i jej wielokrotności; są to liczby 2, 4, 6, 8, 10, 12, 14, … Zobaczmy, jak to będzie wyglądać, gdy liczba kolumn będzie równa właśnie 2:

2	3
4	5
6	7
8	9
…	…

Tabela 7

Podczas zaznaczania tych liczb dociera do nas fakt, że wszystkie one znajdują się w pierwszej kolumnie tabeli 7, a więc możemy zakreślić po prostu całą pierwszą kolumnę, ale bez liczby 2:

2	3
4	5
6	7
8	9
…	…

Tabela 8

Po czym stwierdzamy, że najmniejszą odległością, jaka istnieje między kolejnymi liczbami pierwszymi > 2 jest właśnie 2, gdyż ze względu na nieskończoność liczb pierwszych muszą one wszystkie znajdować się w kolumnie drugiej, a tam liczby występują co druga. Zauważmy, że skoro liczby są rozpisane w dwóch kolumnach, a liczby z pierwszej kolumny zostały zaznaczone (bez 2), więc teraz wśród liczb czytanych

od lewej do prawej, pomijając pierwszy wiersz, z góry na dół, co druga liczba jest **zaznaczona**. Z kolei czytając je kolumnami, zauważamy, że w drugiej kolumnie nie ma ani jednej liczby podzielnej przez 2, a zatem *de facto* wielokrotności liczby 2 zostały **usunięte** z ciągu 2, 3, 4, …

Kolejną liczbą ciągu jest 3. Zaznaczmy więc jej wielokrotności. Pytanie, gdzie mamy je zaznaczyć? Począwszy od liczby 3, czytając co trzecią liczbę, mamy: 6, 9, 12, 15, 18, 21… Jeżeli teraz zaczniemy zaznaczać te liczby w tabeli 7, to przekonamy się, że występują one na przemian, raz w pierwszej kolumnie, a raz w drugiej, więc i w tabeli 8 również tak będzie. Kolejna liczba to 5, a jej wielokrotności to liczby: 10, 15, 20, 25, 30, … W tym przypadku, gdy zaczniemy zaznaczać te liczby w tabeli 7, również zauważamy, że występują one kolejno raz w jednej, a raz w drugiej kolumnie (w tabeli 8 również tak będzie). Zaznaczmy wymienione wielokrotności i przetransponujmy kolumny w rzędy, otrzymując tabelę 9:

2	4	6	8	10	12	14	16	18	20	22	24	26	…
3	5	7	9	11	13	15	17	19	21	23	25	27	…

Tabela 9

Widzimy, że obraz będzie się powoli zacierał, w miarę jak będziemy zaznaczać wielokrotności kolejnych liczb pierwszych, gdyż już po zaznaczeniu wielokrotności liczby 3 różnica między kolejnymi niezaznaczonymi liczbami w wierszu drugim wynosi na przemian raz 2, a raz 4, licząc od liczby 5, co możemy analizować w miarę możliwości. Zaznaczenie wielokrotności liczby 5 wprowadzi jeszcze większe zamieszanie. Natomiast im dalej zapuścimy się w analizie wiersza drugiego, tym większa będzie się pojawiać niepewność ze względu na brak wiedzy. Przypomnijmy bowiem, że na podstawie **twierdzenia 1** znamy jedynie liczby pierwsze nie większe niż 25, gdyż w tabeli 9 największą liczbą pierwszą, jakiej wielokrotności zaznaczyliśmy, jest właśnie liczba 5, więc tylko ten obszar możemy analizować.

Jeżeli rozpiszemy liczby z ciągu 2, 3, 4, … w trzech kolumnach, to bez problemu stwierdzimy, że w pierwszym kroku, tzn. zaznaczając wielokrotności liczby 2 i od niej większe, będziemy zaznaczać na przemian liczby w trzeciej, w pierwszej i w drugiej kolumnie. Natomiast gdy zaznaczymy wielokrotności liczby 3 i od niej samej większe, to widzimy, że wszystkie występują w drugiej kolumnie:

2	3	4
5	6	7
8	9	10
…	…	…

Tabela 10

Wydaje się więc logiczne, by liczby z ciągu 2, 3, 4, … rozpisać w sześciu kolumnach:

2	3	4	5	6	7
8	9	10	11	12	13
14	15	16	17	18	19
…	…	…	…	…	…

Tabela 11

a następnie zaznaczyć w tabeli 11 wielokrotności liczby 2, otrzymując:

2	3	4	5	6	7
8	9	10	11	12	13
14	15	16	17	18	19
…	…	…	…	…	…

Tabela 12

oraz zaznaczyć w tabeli 12 wielokrotności liczb > 3, otrzymując:

2	3	4	5	6	7
8	9	10	11	12	13
14	15	16	17	18	19
...	...	...	...	...	...

Tabela 13

Zaznaczone w tabeli 12 liczby występują w pierwszej, trzeciej i piątej kolumnie, więc bez problemu możemy od razu zaznaczyć całe te kolumny (nie licząc 2), zamiast zaznaczać liczby pojedynczo. Natomiast gdy zaczniemy liczyć od 3 co trzecią liczbę, to szybko zorientujemy się, że zaznaczane liczby pojawiają się na przemian raz w kolumnie piątej, która jest już zaznaczona, a raz w kolumnie drugiej tabeli 12, wypełniając tym samym całą tę kolumnę (bez liczby 3). Otrzymamy w ten sposób tabelę 13. Również i tu możemy zauważyć, że rozpisanie liczb w sześciu kolumnach, z których zaznaczyliśmy pierwszą kolumnę bez liczby 2 oraz drugą bez liczby 3, trzecią oraz piątą, powoduje, że czytane od lewej do prawej, z góry na dół, co druga liczba, licząc od 4, i co trzecia liczba, licząc od 6, jest **zaznaczona**. Mówiąc inaczej, raz co druga, a raz co czwarta liczba, licząc od 5, jest **niezaznaczona**. Z kolei czytając kolumnami, zauważamy, że w czwartej i szóstej kolumnie nie ma ani jednej liczby podzielnej przez 2 i przez 3, a zatem *de facto* wielokrotności liczb 2 i 3 zostały **usunięte** z pierwotnego ciągu. Jest to w gruncie rzeczy podstawa takiego rozpisywania liczb z ciągu 2, 3, 4, … na określoną liczbę kolumn.

Niezaznaczone kolumny 4 i 6 (tabela 13) powinny zawierać pozostałe liczby pierwsze. Jednak co nas uprawnia do tego, by tak twierdzić? Jak na razie to nic. Natomiast z całą pewnością możemy powiedzieć, że nie zawierają one liczb podzielnych przez 2 i 3, gdyż wszystkie wielokrotności zaznaczyliśmy i pokazaliśmy, że znajdują się one w kolumnach 1, 2, 3 i 5. Płynie stąd ważny wniosek, że jedyne wielokrotności kolejnej liczby pierwszej, jakie pozostały nam do usunięcia (a raczej zaznaczenia),

są postaci: $5 \cdot 5$, $5 \cdot 11$, $5 \cdot 17$, ..., tzn. liczba 5 pomnożona przez wszystkie liczby z kolumny 4, oraz $5 \cdot 7$, $5 \cdot 13$, $5 \cdot 19$, ..., czyli liczba 5 pomnożona przez wszystkie liczby z kolumny 6 w tabeli 13. Wszystkie wymienione wielokrotności muszą występować w kolumnach 4 i 6, ponieważ po pierwsze, wielokrotności takie, jak: $5 \cdot 2$, $5 \cdot 8$, $5 \cdot 14$, ..., $5 \cdot 3$, $5 \cdot 9$, $5 \cdot 15$, ... , $5 \cdot 4$, $5 \cdot 10$, $5 \cdot 16$, ... , $5 \cdot 6$, $5 \cdot 12$, $5 \cdot 18$, ..., a więc iloczyny liczby 5 i kolejno wszystkich liczb z kolumn odpowiednio 1, 2, 3, 5 zostały już zaznaczone i występują one właśnie w tych kolumnach. Po drugie, liczby $5 \cdot 5$, $5 \cdot 11$, $5 \cdot 17$, ... można zapisać w postaci $5(6n - 1)$, a liczby $5 \cdot 7$, $5 \cdot 13$, $5 \cdot 19$, ... można zapisać jako $5(6n + 1)$. A te, jak widać, są wszystkie podzielne przez 5 oraz nie są podzielne przez 2 i 3, przez to niemożliwe jest, by występowały w kolumnach 1, 2, 3 lub 5.

Pierwszą niezakreśloną liczbą w tabeli 13 jest kolejna liczba pierwsza równa 5. Jeżeli zaczniemy zaznaczać w tabeli wielokrotności tej liczby, to przekonamy się, że występują one na przemian raz w 4, a raz w 6 kolumnie. Jeśli zaznaczalibyśmy dalej wielokrotności kolejnych liczb pierwszych > 5, to znów zatrzemy możliwość analizowania relacji między pozostałymi liczbami pierwszymi. Zamiast zaznaczać, spróbujmy usunąć te liczby z ciągu 2, 3, 4, 5, ... Rozpisując je w 5 kolumnach, otrzymamy:

2	3	4	5	6
7	8	9	10	11
12	13	14	15	16
...	...	...	...	...

Tabela 14

Zaznaczając co piątą liczbę, licząc od 5, zaznaczymy całą czwartą kolumnę (bez liczby 5) tabeli 14, otrzymując tym sposobem tabelę 15. Jeżeli zaznaczymy w niej wielokrotności liczby 2, to przekonamy się, że pola, na których one występują, tworzą szachownicę, a to utrudnia, wręcz pozbawia

możliwości badania relacji między liczbami pierwszymi. Podobnie jest z wielokrotnościami liczby 3. Żeby tej możliwości nie utracić, liczba kolumn, w których rozpisujemy liczby z ciągu 2, 3, 4, …, powinna być podzielna zarówno przez 2, 3, jak i przez 5. Najmniejszą taką liczbą jest liczba 30. Rozpisując ciąg 2, 3, 4, … w 30 kolumnach oraz zaznaczając w nim wszystkie wielokrotności liczby 2, otrzymujemy tabelę 16.

2	3	4	5	6
7	8	9	10	11
12	13	14	15	16
…	…	…	…	…

Tabela 15

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Tabela 16

Bez najmniejszego problemu możemy stwierdzić, że nasze postępowanie możemy uprościć i zaznaczyć od razu całe kolumny, od pierwszej (bez liczby 2) co drugą kolumnę. Następnie zaznaczamy wszystkie wielokrotności liczby 3 oraz liczby 5 i od nich samych większe w tabeli 16 i w ten sposób otrzymujemy kolejną tabelę 17.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Tabela 17

I znów możemy skrócić to postępowanie, zaznaczając od razu całe kolumny, tj. od drugiej (bez liczby 3) co trzecią kolumnę oraz od czwartej (bez liczby 5) co piątą kolumnę.

Do czego nas to doprowadziło? Czy po zaznaczeniu wymienionych liczb tabela 17 nie wygląda bardziej czytelnie, niż gdybyśmy zrobili to liniowo? Co możemy powiedzieć o tak skonstruowanej tabeli? Przytoczmy kilka faktów. Kolumny, które są niezaznaczone, nie zawierają żadnych wielokrotności liczb 2, 3, 5. Oznacza to, że wielokrotności liczb 2, 3 i 5 zostały **usunięte** z ciągu 2, 3, 4, ... Liczby, które zaznaczamy, tworzą kolumny, *ergo* zamiast zaznaczać liczby, możemy zaznaczyć całe kolumny. Również i tu możemy zauważyć, że spośród liczb rozpisanych w 30 kolumnach, czytanych od lewej do prawej, z góry na dół, co druga, licząc od 4, co trzecia, licząc od 6, oraz co piąta, licząc od 10, jest **zaznaczona**. Lub prościej: co czwarta, co druga, co czwarta, co druga, po czym co szósta, co druga i co szósta, licząc od liczby 7 jest **niezaznaczona**. Mamy taką **sekwencję** liczb, która się powtarza już od wiersza drugiego, tzn. od liczby 31: 6, 4, 2, 4, 2, 4, 6, 2, co może nam się przydać przy rozważaniu odległości między kolejnymi liczbami pierwszymi. Niezaznaczone kolumny powinny zawierać pozostałe liczby pierwsze. Rozpatrując kolumny w tabeli 17, widzimy, że liczby w kolumnie pierwszej, tzn. liczby 2, 32, 62, …, tworzą ciąg arytmetyczny, który można zapisać w postaci wzoru ogólnego $30n - 28$. Mając taki wzór, bez problemu zauważamy, czemu ten ciąg wyznacza liczby podzielne przez 2. Bowiem $30n - 28 = 2(15n - 14)$, a wyrażenie z prawej strony tej równości podzielne jest właśnie przez 2. Podążając tym śladem, znajdziemy wzory ogólne dla pozostałych liczb występujących w kolejnych kolumnach. Te, które nie zostały zaznaczone, np. liczby z kolumny 28, tzn. liczby 29, 59, 89, ..., tworzą ciąg arytmetyczny, który można zapisać w postaci wzoru ogólnego $30n - 1$. A ten, jak i pozostałe niezaznaczone ciągi, ma tę własność, że nie możemy wyciągnąć żadnej liczby naturalnej > 1 przed nawias, tym samym nie możemy stwierdzić, ile liczb pierwszych, a ile złożonych wyznaczają te ciągi. Gdybyśmy teraz chcieli usunąć, a nie tylko zaznaczyć wielokrotności kolejnej liczby pierwszej > 7 z tabeli 17, to żeby nie zatracić możliwości badania,

np. odległości między tymi liczbami, rozsądne wydaje się, żeby rozpisać ciąg 2, 3, 4, … w $30 \cdot 7 = 210$ kolumnach, co już przysporzyłoby nam niemałych problemów. A przecież to dopiero początek.

Dalej stwierdzamy, że najmniejszą niezakreśloną liczbą (tabela 17) jest kolejna liczba pierwsza równa 7, a najmniejszą liczbą złożoną jest liczba 49, co oznacza, że między tymi liczbami wszystkie są pierwsze. Wiemy również, że skoro zaznaczając liczby, usunęliśmy wszystkie wielokrotności trzech kolejnych liczb pierwszych $2 \cdot k$, $3 \cdot k$, $5 \cdot k$, więc pozostałe, jakie należy zaznaczyć, to nie tylko $7 \cdot 7$, ale również $7 \cdot 11$, $7 \cdot 13$, $7 \cdot 17$, $7 \cdot 19$, $7 \cdot 23$, …, tzn. liczbę 7 mnożymy przez liczby, które są niezaznaczone i występują w kolejnych kolumnach czytane od lewej do prawej. Widzimy, że gdy zaznaczymy cztery liczby w omawianej tabeli, tj. liczby $7 \cdot 7 = 49$, $7 \cdot 11 = 77$, $7 \cdot 13 = 91$, $7 \cdot 17 = 119$, to pierwszą niezaznaczoną jest kolejna liczba pierwsza równa 11, co bez zaznaczania tych czterech liczb mogliśmy już stwierdzić. I teraz najmniejszą liczbą złożoną jest liczba 121. A zatem z **twierdzenia 1** wnosimy, że wszystkie pozostałe < 121 i niezakreślone liczby są liczbami pierwszymi. Zauważmy, jak dużo jest liczb w niezakreślonych kolumnach. Aż do liczby 121 jest ich 8 kolumn po 4 liczby w każdej, co nam daje 32 liczby. Zaznaczymy jedynie 5 i wiemy, że pozostałe są pierwsze. Zatem od 32 wystarczy odjąć 5 i już wiemy, że liczb pierwszych między 7 a 121 jest 27. Dodając trzy pierwsze, tzn. liczby 2, 3 i 5, od których zaczęliśmy nasze postępowanie, uzyskujemy 30 liczb pierwszych z przedziału od 2 do 121. Zauważmy też, że wyłania się tu pewna idea, w jaki sposób można rozwiązać zagadnienia związane z liczbami pierwszymi bliźniaczymi. Widzimy, że np. w kolumnach 10 i 12, 16 i 18 oraz 28 i 30 (tabela 17) mogą takie liczby występować. Możemy też obliczyć, ile jest tych liczb w przybliżeniu. Bo skoro już wiemy, że liczb pierwszych od 7 do 121 jest 27, a liczb w kolumnach jest 6 po cztery w każdej, razem 24, więc zakładając, że te 5 liczb złożonych wypadnie akurat w tych kolumnach, otrzymamy 19 liczb pierwszych. Bez względu na to, jak one się rozłożyły, musimy również odrzucić liczby pierwsze, które są do pary dla zaznaczonych liczb, np. dla liczby 49 musimy odrzucić liczbę 47,

liczbę 79 jako kandydata na liczbę bliźniaczą odrzucamy, gdyż jej liczba do pary, tzn. liczba 77, będąc liczbą złożoną została zakreślona itd. Tak więc mając 5 liczb złożonych, musimy odrzucić w sumie 10 liczb. A zatem, mając 24 liczby i odejmując od nich 10, otrzymamy 14 liczb pierwszych, z których połowa musi być postaci p, a druga połowa postaci $p + 2$. W istocie tych liczb jest tam więcej, konkretnie 16. W tabeli 18 na szaro zaznaczono liczby, które można wykluczyć drogą samego tylko obliczania, a nie faktycznego zaznaczania.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Tabela 18

Czy powyższe argumenty są wystarczające, by sądzić, że faktycznie warto zagłębiać się coraz dalej w analizę algorytmu Eratostenesa? Zauważmy, że liczby w powstałych kolumnach tworzą ciągi arytmetyczne, a te mają współczynnik kierunkowy, wyraz wolny, dziedzinę i przeciwdziedzinę. Pójdźmy więc w tym kierunku i przekonajmy się. Zaprezentowane rozpisywanie liczb w kolumnach można potraktować jako przypadek szczególny. Żeby natomiast przejść do ogólnej postaci tego rozumowania, musimy zdobyć większą wiedzę na temat tak skonstruowanego ciągu liczb 2, 3, 4, … Zachodzą tu **trzy aspekty**. Pierwszy, to rozpisanie tego ciągu na pewną liczbę kolumn, czym zajmiemy się w następnym rozdziale „Podział przestrzeni". Pozostałe dwa omówimy w rozdziałach „Konstrukcja przestrzeni – część 1" i „Konstrukcja przestrzeni – część 2".