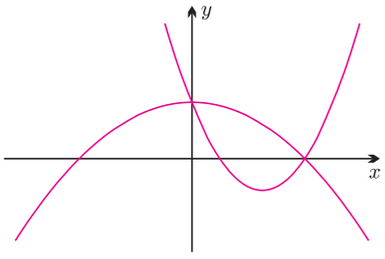
Od paraboli do podziału sekretu

Tomasz KAZANA[*]

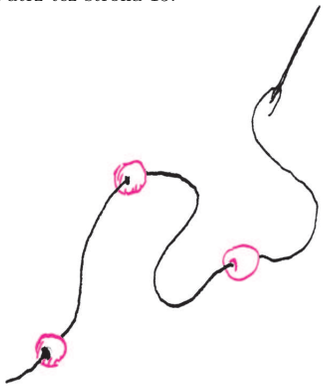


Zaczniemy od przypomnienia kilku podstawowych własności wielomianów nad liczbami rzeczywistymi. Skupmy się najpierw na funkcji kwadratowej $f(x) = ax^2 + bx + c$. Będzie nas interesowało to, ile *informacji* potrzebujemy, żeby ustalić parametry a, b i c. Na przykład, jeśli znamy dwa punkty $P = (x_1, y_1)$, $Q = (x_2, y_2)$, przez które przechodzi szukana „szkolna" parabola, to wiemy jeszcze *zbyt mało*. Co to znaczy? Weźmy dla przykładu $P = (0, 1)$ oraz $Q = (2, 0)$. Łatwo sprawdzić, że zarówno funkcja $f_1(x) = -\frac{1}{4}x^2 + 1$, jak i $f_2(x) = x^2 - \frac{5}{2}x + 1$ spełniają nasze oczekiwania, tzn. oba punkty leżą na wykresach obu funkcji. Okazuje się, że zawężenie kryteriów do trzech punktów sprawia, iż znajdziemy co najwyżej jedno rozwiązanie. Faktu tego nie będziemy ściśle dowodzić, intuicja powinna jednak podpowiadać, że właśnie trzy punkty są konieczne i wystarczające. Dlaczego? Jeden punkt przekłada się na jedno równanie liniowe z trzema niewiadomymi a, b, c. Trzy takie punkty dają trzy równania.

Podana wyżej własność funkcji kwadratowej uogólnia się na wielomiany wyższych stopni. Sformułujemy odpowiednie twierdzenie.

Twierdzenie 1. *Jeśli liczby rzeczywiste $x_1, x_2, \ldots, x_{n+1}$ są parami różne, to przez ustalone punkty $P_1 = (x_1, y_1), P_2 = (x_2, y_2), \ldots, P_{n+1} = (x_{n+1}, y_{n+1})$ przechodzi wykres dokładnie jednego wielomianu nad liczbami rzeczywistymi stopnia co najwyżej n.*

Patrz też strona 15.



Możemy to uogólnić. Otóż twierdzenie jest wciąż prawdziwe, jeśli zmienimy zbiór, nad którym rozpatrywane są wielomiany. Przykładowo, w świecie liczb zespolonych to również jest prawdą. Dla osób zaznajomionych z podstawami algebry będzie jasne, jeśli powiemy, że jest ono prawdziwe nad każdym *ciałem*. Dla naszych rozważań nie będzie potrzebna dokładna definicja tej struktury. Zajmiemy się jednym konkretnym przykładem. Otóż niech p będzie liczbą pierwszą oraz niech $\mathbb{Z}_p$ będzie zbiorem liczb naturalnych od 0 do $p-1$. Skojarzymy z tym zbiorem działania dodawania i mnożenia. Przyjmiemy, że aby dodać dwie liczby z tego zbioru, dodajemy je w sposób tradycyjny, po czym jako wynik bierzemy resztę z dzielenia przez p. Dla mnożenia robimy analogicznie. Poniższy przykład ilustruje te definicje dla $p = 13$:

$$3 + 11 = 1, \qquad 4 \cdot 6 = 11, \qquad 9 \cdot 9 + 10 = 0.$$

Nad taką dziwaczną strukturą będziemy badać tradycyjne wielomiany. Ponownie przyjmijmy $p = 13$ oraz $w_1(x) = x^3 + 2x^2 + 6$, $w_2(x) = x^5 + 3$, $w_3(x) = x + 4$. Mamy wówczas przykładowo:

$$w_1(4) = 11, \quad w_2(4) = 0, \quad w_3(10) = 1.$$

Jak uprzedziliśmy, w tym świecie również zachodzi twierdzenie o wielomianach.

Twierdzenie 2. *Jeśli elementy ciała $x_1, x_2, \ldots, x_{n+1} \in \mathbb{Z}_p$ są parami różne, to przez ustalone punkty $P_1 = (x_1, y_1), P_2 = (x_2, y_2), \ldots, P_{n+1} = (x_{n+1}, y_{n+1})$ przechodzi wykres dokładnie jednego wielomianu nad $\mathbb{Z}_p$ stopnia co najwyżej n, o ile $n < p$.*

A gdzie w tym wszystkim podział sekretu? Jeszcze chwila cierpliwości i wszystko się wyjaśni. Mamy już potrzebny aparat matematyczny, czas więc na ogólne wprowadzenie w problematykę sekretów, spisków i wzajemnej nieufności.

Rozważmy uproszczoną sytuację: pewna grupa k osób ma jakiś wspólny sekret M, który interpretujemy jako jedną liczbę z zakresu $0, \ldots, p-1$, czy raczej – mówiąc językiem algebry – jako element ciała $\mathbb{Z}_p$. Chcemy jakoś *rozdzielić* informację o M wśród grupy, aby uzyskać następujący poziom bezpieczeństwa sekretu M.

Rozwiązanie zadania M 1305.
Rozważmy planszę o wymiarach $m \times n$ i na każdym polu dokonajmy losowania: z prawdopodobieństwem x postawimy tam biały pionek, a z prawdopodobieństwem $y = 1 - x$ – czarny. Wówczas prawdopodobieństwo tego, że na każdym z m pól wybranej kolumny stoi biały pionek, jest równe x^m. W takim razie $1 - x^m$ to prawdopodobieństwo tego, że w tej kolumnie znajdzie się chociaż jeden pionek czarny, a $(1 - x^m)^n$ możemy zinterpretować jako szansę na to, że w każdej kolumnie będzie przynajmniej jeden czarny pionek. Podobnie $(1 - y^n)^m$ to szansa zdarzenia, że w każdym wierszu jest co najmniej jeden biały pionek. Zauważmy jednak, że któreś z tych zdarzeń musi wystąpić, ponieważ jeżeli jakaś kolumna zawiera same białe pionki, to w każdym wierszu jest już biały pionek. To dowodzi podanej nierówności.

[*]Instytut Informatyki,
Uniwersytet Warszawski

Poziom bezpieczeństwa 1. *Dowolna podgrupa licząca $k-1$ osób nie jest w stanie odtworzyć sekretu M na podstawie informacji posiadanych przez członków podgrupy. Pełna grupa k osób jest w stanie odtworzyć M.*

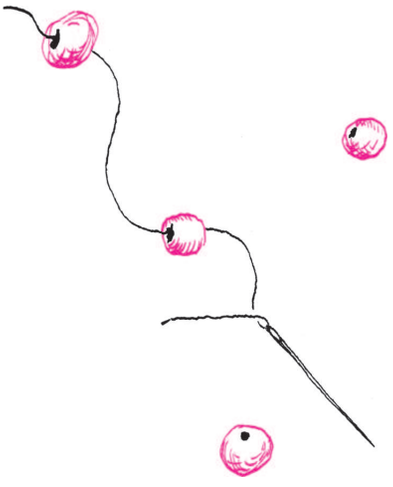
Wróćmy do świata wielomianów. Niech W będzie losowym wielomianem nad $\mathbb{Z}_p$ stopnia $k-1$, takim że $W(0)=M$. Tylko ten wielomian będzie nam potrzebny, aby rozdzielić sekret. Pierwszej osobie zdradzimy wartość $W(1)$, drugiej – $W(2)$ itd. Ostatnia osoba pozna $W(k)$. Teraz z twierdzenia 2 wynika, że informacje posiadane przez te osoby pozwalają odtworzyć wielomian, a więc i obliczyć $W(0)$, to znaczy poznać sekret M. Gdy zabraknie choć jednej osoby, to wielomian nie jest wyznaczony jednoznacznie i wiadomość pozostaje tajna.

Poziom bezpieczeństwa 1 da się uzyskać znacznie prościej, niż opisano to w artykule. Wystarczy pierwszym $k-1$ osobom przydzielić losowe liczby ℓ_i, a ostatniej liczbę

$$M-\sum_{i=1}^{k-1}\ell_i.$$

Jednak pomysł wykorzystujący własności wielomianów uogólnia się na inne problemy (np. te podane w dalszej części artykułu), których nie da się rozwiązać aż tak trywialnie.

Co tu jest jeszcze do dowiedzenia? Powyższe rozumowanie zawiera, oczywiście, pewne uproszczenia. W szczególności nie wskazaliśmy, jak wykazać, że żadne $k-1$ osób nie może odtworzyć M. Nie będziemy wszystkiego uzupełniać. Chcemy jednak dokładnie określić, czego należałoby ściśle dowieść, aby móc stwierdzić, że opisany schemat jest *bezpieczny*.



Przede wszystkim nie zdefiniowaliśmy precyzyjnie, co rozumiemy przez sformułowanie, że wiadomość jest tajna. Nie wystarczy powiedzieć, że posiadana wiedza nie wystarcza do jednoznacznego odtworzenia sekretu M. Mogłoby się przecież tak zdarzyć, że – w skrajnym przypadku – niejednoznaczność polega na tym, iż mamy dwóch kandydatów na M. Pierwsze przybliżenie definicji mogłoby więc iść w tę właśnie stronę. To znaczy chcielibyśmy, aby posiadana wiedza nie mogła wykluczyć żadnego kandydata na M. Jednak również i taka definicja jest za słaba. Nie wyklucza bowiem przypadku, gdy posiadana wiedza pozwala stwierdzić, że, na przykład, $M=23821$ z prawdopodobieństwem 0,9 (a nie $\frac{1}{p}$, jak pewnie byśmy oczekiwali). Najsilniejsza definicja jest sformułowana właśnie w języku probabilistyki: dana wiadomość jest tajna, jeśli posiadana wiedza nie pozwala na ustalenie innego rozkładu prawdopodobieństw tajnego sekretu niż rozkład jednostajny.

Okazuje się, że dzielenie sekretu za pomocą wielomianu spełnia tę najsilniejszą definicję. Zachęcamy do udowodnienia tego faktu, a przynajmniej dokładnego sformułowania, co tak naprawdę trzeba udowodnić.

Dalsze zastosowania. Wielomiany dają nam jeszcze inne ciekawe możliwości (ponownie k oznacza liczbę osób).

Poziom bezpieczeństwa 2. *Dowolna podgrupa $k-4$ osób nie jest w stanie odtworzyć M. Każda podgrupa $k-3$ osób jest w stanie odtworzyć sekret.*

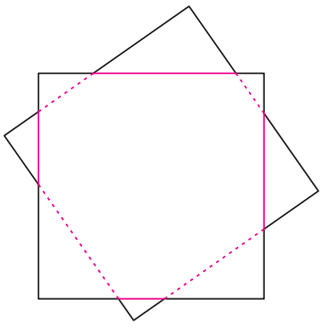
Powyższe bezpieczeństwo uzyskujemy, na przykład, następująco: losujemy wielomian stopnia $k-4$ o wartości M w zerze. Osobom dajemy kolejne wartości $W(1),W(2),\ldots,W(k)$. Ponownie twierdzenie 2 dowodzi tezy. Liczba 4 została tu wybrana przykładowo, można wybrać dowolną inną. Oczywiście, żeby zachować pełną ścisłość, należy udowodnić trudniejszy fakt dotyczący rozkładu prawdopodobieństw.

To jednak nie koniec. Jako ostatnią rzecz proponujemy ćwiczenie. Zachęcamy Czytelnika do pokazania, jak użyć techniki wielomianów, aby osiągnąć następujący poziom bezpieczeństwa (dla Czytelnika Leniwego rozwiązanie jest w numerze).

Poziom bezpieczeństwa 3. *Niech k oznacza liczbę pięcioosobowych rozłącznych grup osób. Chcemy, aby do poznania sekretu konieczna była większość (a więc co najmniej trzy osoby) z co najmniej $\frac{k}{2}$ grup.*

Opisany w artykule pomysł dzielenia sekretu zawdzięczamy izraelskiemu kryptografowi Adiemu Shamirowi. Zainteresowanych zachęcamy do samodzielnych poszukiwań i dalszego zgłębiania tej tematyki.

Rozwiązanie zadania M 1303.
Zauważmy, że oprócz ośmiokąta powstało osiem podobnych trójkątów,



w każdym z których stosunek sumy długości przyprostokątnych do długości przeciwprostokątnej jest równy α. Oznaczając sumę długości kolorowych odcinków ciągłych przez x, a przerywanych przez y, widać, że obwód jednego kwadratu jest równy $x+\alpha y$, a drugiego $y+\alpha x$, co po przyrównaniu daje $x=y$.