Ministerstwo Nauki i Szkolnictwa Wyższego

dla każdego matematyka, który chciałby się zapoznać z prezentowaną dziedziną, a takich, szczególnie wśród topologów, jest wielu.

Przejdę teraz do krótkiego omówienia treści książki. Ponieważ prezentowana jest teoria 3-rozmaitości w kategorii PL, pierwszy rozdział jest poświęcony topologii kawałkami liniowej. Jest on wybitnie informacyjny. Twierdzenia podane są bez dowodów.

W rozdziałach II–V jest przedstawiona klasyczna już część teorii 3-rozmaitości. Rozdział II – rozkłady Heegaarda, rozdział III – twierdzenia o pętli, o sferze i lemat Dehna. Rozdziały te opracowane są wyraźnie na podstawie książki J. Hempla *3-manifolds*; nie są jednak, oczywiście, prostym tłumaczeniem – niewielka część materiału z odpowiednich rozdziałów książki Hempla została pominięta. Pojawiają się natomiast ilustracje, ćwiczenia i twierdzenia, których u Hempla nie ma. Materiał poszerzony jest o nowe rezultaty, takie jak twierdzenie Bonahona–Hodsona (bez dowodu) czy paragraf poświęcony niezmienniczym wersjom twierdzeń o pętli, o sferze i niezmienniczemu lematowi Dehna.

Rozdział IV dotyczy rozkładu rozmaitości 3-wymiarowych na sumę spójną. Wykazano, że każda zwarta 3-rozmaitość może być przedstawiona jako skończona suma rozmaitości pierwszych (tw. Knesera) i rozkład ten jest jednoznaczny (tw. Hakena, Milnora) oraz omówiono rozkład 3-rozmaitości wzdłuż dysku. Rozdział V poświęcony jest powierzchniom nieściśnialnym.

Następny rozdział zawiera krótki zarys teorii węzłów. Można go polecić studentom, pragnącym zapoznać się z elementami tej teorii bez konieczności wertowania całej książki. Omawiane są: grupa węzła, powierzchnie Seiferta, klasyczny wielomian Alexandera oraz łatwy do wyznaczenia wielomian Conwaya. O ile wiem, w przygotowaniu jest nowy skrypt J. H. Przytyckiego *Teoria węzłów*. Nie ukaże się on jednak zbyt prędko.

Znajomość pewnych elementów teorii węzłów przydatna jest przy czytaniu rozdziału VII (Działania grup skończonych na $S^3$), jedynego, w którym rozważane są rozmaitości gładkie, rozdziału VIII (Chirurgie Dehna na rozmaitościach 3-wymiarowych) i rozdziału IX (Związek pomiędzy topologią 3- i 4-wymiarową), w którym omówiony jest m.in. rachunek splotów Kirby'ego.

Pozostały rozdział X (Triangulacja 3-rozmaitości) zawiera dowód podanego już w rozdziale I twierdzenia 2.1, mówiącego właśnie o triangulowalności 3-rozmaitości.

Zaletą skryptu jest duża ilość ćwiczeń, przykładów i ilustracji oraz obszerna bibliografia. Natomiast, jak to bywa zazwyczaj w skryptach, brak jest skorowidzów nazw i symboli. Zdarzają się też usterki redakcyjne, takie jak błędy korektorskie (np. braki litery lub nawiasu), niekonsekwencje w oznaczeniach (np. macierz transponowana bywa oznaczana $A^T$, $A^t$ lub $A'$) i trochę większe niedokładności (np. na str. $161^{10}$).

Nie ma jednak tych usterek tak dużo, aby w istotny sposób utrudniały studiowanie tekstu. Mam też zastrzeżenie natury leksykalnej w stosunku do tytułu. Powinien chyba brzmieć „Topologia trójwymiarowych rozmaitości", a nie „Topologia trzywymiarowych rozmaitości".

Podsumowując, uważam, że skrypt jest pozycją bardzo cenną.

*Witold Rosicki*

## Neal Koblitz, *A course in number theory and cryptography*, Graduate Texts in Mathematics 114, Springer-Verlag, New York 1987, str. 208, ISBN 0-387-96576-9, ISBN 3-540-96576-9.

Autor dał się poznać jako świetny popularyzator różnych działów matematyki związanych z teorią liczb. Napisał kilka atrakcyjnych książek.

Na przykład, szeroko znana jest jego książka poświęcona analizie niearchimedesowskiej, która mimo niedużej objętości wprowadza czytelnika w zasadnicze wyniki,

metody i idee tej dziedziny; przy tym autor na ogół nie opuszcza dowodów, lecz często przenosi je do zadań. Wykład prowadzony jest na wysokim poziomie naukowym, lecz równocześnie autor dba stale o utrzymywanie zainteresowania czytelnika tematem, stosując różne pomysłowe ujęcia. Książka tego typu nie zastępuje monografii zawierającej systematyczny i kompletny wykład przedmiotu, lecz za to przyciąga i budzi zainteresowanie szerokiego grona matematyków niespecjalistów w danej dziedzinie, którzy by się nie zabrali do studiowania monografii.

Podobny charakter ma również recenzowana książka poświęcona związkom teorii liczb z kryptografią. Autor przedstawił kilka zagadnień z teorii liczb, które znajdują zastosowania w kryptografii. Zrobił to po mistrzowsku: Na niewielu stronach podał kompletne i przejrzyste dowody potrzebnych mu faktów, ilustrując je trafnie dobranymi przykładami umieszczonymi często w zadaniach. Przy tym oczywiście opuścił trudne dowody kilku zasadniczych twierdzeń.

Po przeczytaniu tekstu i rozwiązaniu zadań czytelnik ma podstawowe informacje i rozumie dokładnie omawiane zagadnienia, a także potrafi zastosować poznaną teorię w prostych sytuacjach.

Następnie autor przedstawił podstawowe metody stosowane w kryptografii oparte na podanych wcześniej wiadomościach z teorii liczb.

Omówimy pokrótce treść poszczególnych rozdziałów. W rozdziałach I, II, V i VI zebrane są wiadomości z teorii liczb i algebry, które są wykorzystywane w rozdziałach III i IV poświęconych kryptografii.

Dokładniej, w poszczególnych rozdziałach przedstawione są następujące zagadnienia. Rozdział I. Wykonywanie działań na liczbach zapisanych w różnych układach numeracji, kongruencje, twierdzenie chińskie o resztach. Rozdział II. Opis ciał skończonych i ich grupy multyplikatywnej, wielomiany nierozkładalne nad ciałami skończonymi, reszty kwadratowe, symbole Legendre'a i Jacobiego, prawo wzajemności dla reszt kwadratowych z dowodem za pomocą sum Gaussa w ciałach skończonych.

Rozdział III. Najprostsze metody szyfrowania tekstów polegające na permutowaniu zbioru liter lub par liter, które odpowiada przekształceniu afinicznemu na prostej lub płaszczyźnie. Łamanie takiego szyfru za pomocą badania najczęściej występujących liter lub par liter. Przykłady wzięte z języka angielskiego i rosyjskiego. Rozdział IV. Przesyłanie zaszyfrowanych wiadomości, posługując się tylko jawną korespondencją. Omówimy później dokładniej ten rozdział.

Rozdział V. Warunki konieczne na to, by liczba była pierwsza, liczby pseudopierwsze i różne ich uogólnienia. Szczegółowo omówione są pewne odkryte niedawno warunki konieczne pierwszości liczb (Solovay-Strassen, Miller–Rabin, Adleman–Pomerance–Rumely, Cohen–Lenstra). Metody rozkładania dużych liczb na czynniki pierwsze: Metoda Monte Carlo, przedstawianie w postaci różnicy dwóch kwadratów, metoda małych reszt kwadratowych i zastosowanie do niej ułamków łańcuchowych.

Rozdział VI. Grupa punktów wymiernych na krzywej eliptycznej. Liczba tych punktów na krzywej eliptycznej określonej nad ciałem skończonym. Bez dowodu, twierdzenie Hassego podające oszacowanie tej liczby i twierdzenie Deligne'a o postaci funkcji $\zeta$ krzywej eliptycznej.

Przy końcu każdego paragrafu umieszczono sporo zadań (szczegółowe ich rozwiązania podane są przy końcu książki) oraz kilka pozycji bibliograficznych (na ogół z ostatnich lat). Liczne zadania zawierają teksty, które czytelnik ma zaszyfrować lub odszyfrować.

Najbardziej atrakcyjnym rozdziałem jest rozdział IV poświęcony takim metodom szyfrowania, które pozwalają przesyłać informacje w jawnej korespondencji bez obaw o ich ujawnienie. Zapewne ten rozdział był pretekstem do napisania całej książki.

Dawniej osoby używające szyfru w korespondencji posługiwały się tajnym kluczem znanym im obu. Osoby postronne mające dostęp do zaszyfrowanego tekstu nie mogły go odszyfrować, gdyż nie znały klucza.

Około 10 lat temu zauważono, że można obyć się bez tajnego klucza znanego *obu* osobom stosującym szyfr. Przy tym osoby te mogą przesyłać wszystkie informacje między

sobą *jawnie*, a mimo to są w stanie przesyłać wiadomości, których żadna postronna osoba nie rozszyfruje.

Zasada jest prosta. Osoba $A$ chce przesłać osobie $B$ wiadomość w postaci liczby $x$ należącej do pewnego zbioru $X$ znanego obu osobom. W tym celu $A$ ustala pewne odwzorowanie wzajemnie jednoznaczne $f\colon X \to X$, a osoba $B$ ustala swoje odwzorowanie $g\colon X \to X$. Przy tym funkcja $f$ znana jest tylko osobie $A$, a funkcja $g$ – tylko osobie $B$. Zakładamy przy tym, że wyboru tych funkcji $f, g$ dokonuje się w sposób, który gwarantuje, że ich złożenie będzie przemienne, tzn. $fg = gf$.

Następnie osoba $A$ przesyła jawnie osobie $B$ liczbę $f(x)$. Oczywiście, $B$ nie może odczytać stąd $x$, bo nie zna $f$. Nie martwi się tym jednak, lecz przesyła jawnie osobie $A$ liczbę $g(f(x)) = f(g(x))$. Teraz $A$ oblicza $f^{-1}(f(g(x))) = g(x)$ i przesyła wynik $g(x)$ do $B$. Tym razem osoba $B$ może odczytać liczbę $x$ obliczając $g^{-1}(g(x)) = x$.

W ten sposób osoba $A$ przekazała osobie $B$ liczbę $x$. Natomiast osoby postronne znają tylko liczby $f(x)$, $g(f(x))$ i $g(x)$, lecz nie znając funkcji $f$ ani $g$ nie mogą poznać liczby $x$.

Tę ideę ogólną można na przykład zrealizować następująco. Obieramy dużą (np. 100-cyfrową) liczbę pierwszą $p$, w każdym razie większą od $x$. Liczbę tę możemy ujawnić osobom postronnym!

Osoby $A$ i $B$ ustalają odpowiednio liczby $a$ i $b$ (duże!) względnie pierwsze z $p-1$. Wtedy funkcje $f$ i $g$ określone za pomocą wzorów

$$f(t) \equiv t^a \pmod{p}, \qquad g(t) \equiv t^b \pmod{p}$$

są odwzorowaniami wzajemnie jednoznacznymi zbioru liczb $1, 2, \ldots, p-1$ i spełniają $fg = gf$. Właśnie tymi funkcjami mogą posłużyć się osoby $A$ i $B$.

Osoby postronne znają tylko reszty z dzielenia przez $p$ liczb $x^a$, $x^{ab}$ i $x^b$, lecz nie znając liczby $a$ ani $b$ nie są w stanie odnaleźć $x$. Wprawdzie mogą obliczać kolejne potęgi liczby $x^a$ chcąc otrzymać $x^{ab}$ (i w ten sposób poznać $b$), lecz jest to praktycznie niemożliwe, ponieważ liczba $b$ jest duża. Nie jest przy tym znany żaden inny algorytm prowadzący szybciej do celu.

Tę samą ideę można zrealizować zastępując grupę multyplikatywną niezerowych reszt z dzielenia przez $p$ grupą punktów wymiernych na krzywej eliptycznej określonej nad ciałem $p$-elementowym. Tu wykorzystuje się trudność polegającą na tym, że znając pewną wielokrotność $aP$ punktu $P$ przy dużym i nieznanym $a$ praktycznie nie sposób jest znaleźć punkt $P$.

Właściwie każdy algorytm występujący w matematyce wymagający dużych rachunków (i nie dający się ominąć w prosty sposób!) może być podobnie użyty w kryptografii.

Autor przedstawia jeszcze inne sposoby przekazywania zaszyfrowanej informacji w jawnej korespondencji. Na przykład metodę opartą na trudności w znalezieniu rozkładu na czynniki liczby będącej iloczynem dwóch dużych (lecz nie znanych!) liczb pierwszych.

Ograniczona objętość recenzji nie pozwala mi jednak na omówienie szczegółowe innych interesujących metod przedstawionych w książce. Mam nadzieję, że zainteresowany czytelnik sięgnie do książki.

Na zakończenie jeszcze dwie uwagi:

1) Autor używa różnych skutecznych sposobów dla zaintrygowania czytelnika. Na przykład opowiada kawał o lekarzach francuskich, radzieckich i amerykańskich. Przy tym wypowiedzi lekarzy francuskich i radzieckich przytacza, a wypowiedź lekarzy amerykańskich podaje w postaci zaszyfrowanej. Czytelnik chcąc poznać pointę musi złamać szyfr.

2) Wydawca pisze: *Text prepared by the author in camera-ready form.* W wyniku tego w książce nie ma błędów drukarskich (bo ich być nie może!). Ponieważ autor jest bardzo staranny, więc również trudno jest znaleźć błędy autorskie. Dostrzegłem tylko jeden: Na str. $99^6$ powinno być $2^{18} \equiv -1 \pmod{37}$.

Uważam, że polskie tłumaczenie tej książki znalazłoby licznych czytelników.

*Jerzy Browkin*