Wszechświat liczb
2. Układ całkowity
Kodowanie i szyfrowanie asymetryczne
skrypt warsztatowy

spisał: Michał Korch

6 maja 2017

Na rozgrzewkę!

Każdy z Was pewnie bawił się w szyfrowanie prostych wiadomości, głównie dla zabawy. Takie proste szyfry można przy odrobinie wysiłku odszyfrować nawet nie znając zasad, wedle których zostały zaszyfrowane. Dlatego może lepiej o nich mówić, że to kodowanie. Niemniej niekiedy robią się z tego niezłe łamigłówki. Spróbujcie rozszyfrować napis na załączonej kartce.

W razie czego pewne wskazówki możecie uzyskać u prowadzącego!

Użyto tu alfabetu bez polskich znaków, za to z q, v i x.

Trochę podzielności

Sprawdźcie, czy: $1 \equiv 0 \pmod 2$, $-2 \equiv 15 \pmod{13}$, $1 \equiv 7^{10} + 8 \pmod 7$, $2 \equiv 2789393 \pmod 5$, $4385 \equiv -39 \pmod{56}$, $-2^{2015} \equiv 0 \pmod{32}$, $3^{3^{723}} + 723 \equiv 0 \pmod 3$.

Sprawdź, czy $3^{2015} + 3^{2016} + 3^{2017}$ jest podzielne przez 13, a $7^{2015} - 7^{2014} + 7^{2016}$ przez 5.

Ile wynosi reszta z dzielenia przez 13 liczb 2^{2015} i 3^{2015}?

Reguły podzielności

Na wykładzie uzasadniliśmy regułę podzielności dla 3 (suma cyfr) i wyprowadziliśmy dużo bardziej skomplikowaną regułę dla 7 (suma cyfr pomnożonych przez cyklicznie występujące współczynniki). Znajdźcie analogiczną regułę dla podzielności przez 11.

Małe Twierdzenie Fermata

Małe Twierdzenie Fermata mówi, że jeśli p jest liczbą pierwszą, i nie dzieli liczby a, to

$$a^{p-1} \equiv 1 \pmod p.$$

Korzystając z Małego Twierdzenia Fermata, udowodnij, że:

- $10^{22} \equiv 1 \pmod{23}$
- $36^6 \equiv 1 \pmod 7$

Szyfrowanie RSA

Szyfrowanie niesymetryczne polega na tym, że są takie problemy, które bardzo trudno rozwiązać. Każda osoba jest wyposażona w dwa klucze: publiczny i prywatny. Klucz publiczny, który służy do szyfrowania wiadomości, jest powszechnie dostępny, ale szalenie trudno (tysiące lat obliczeń) jest z niego wyliczyć klucz prywatny, który właściciel trzyma w tajemnicy. Tylko mając klucz prywatny da się odszyfrować wiadomość zaszyfrowaną kluczem publicznym.

Szyfrowanie RSA wykorzystuje fakt, że bardzo trudno jest rozłożyć dużą liczbę na czynniki pierwsze. Upraszczając nieco sytuację (za chwilę przeprowadzimy symulację), kluczem publicznym jest pewna liczba n będąca iloczynem dwóch liczb pierwszych p i q, zaś p i q będą kluczem prywatnym. To szyfrowanie w algorytmie szyfrowania i odszyfrowywania wykorzystuje właśnie Małe Twierdzenie Fermata.

Podzielcie się na dwie grupy i niech każda z Was weźmie arkusz do symulacji RSA. Zaszyfrujcie krótką wiadomość zgodnie z poleceniami z arkusza, wymieńcie się nimi i je odszyfrujcie. W razie wątpliwości pytajcie prowadzącego.