co jest tym samym wynikiem, który otrzymaliśmy bezpośrednio z definicji. Stosując tę metodę, można samodzielnie sprawdzić, że $\phi(100) = 40$, a więc wynika stąd na przykład, że 7^{40} to 1 modulo 100. Jednak, jak już widzieliśmy, najmniejszą potęgą 7, która daje resztę 1, nie jest 40, a jej dzielnik 4.

Wszystko to służy wskazaniu, że liczba wysłana przez Boba do Alicji, m^e modulo n, może być obliczona bez zbytniego wysiłku na komputerze Boba. Jednocześnie liczby, z którymi mamy do czynienia w praktyce, są bardzo wielkie, więc wyjaśnienie służy pokazaniu, że da się je obsługiwać. Z wielkimi potęgami, z którymi mamy do czynienia, obliczając m^e, można sobie poradzić etapami w procesie znanym jako *szybkie potęgowanie*. Bez wchodzenia w szczegóły: metoda ta obejmuje kolejne podnoszenie do kwadratu i mnożenie potęg, aby otrzymać m^e modulo n przy binarnej postaci e kierującej algorytmem, aby szybko, w kilku krokach, znaleźć potrzebną resztę.

Euklides pokazuje Alicji, jak znaleźć jej liczbę odszyfrowującą

Odszyfrowywanie liczby to magiczna różdżka odbiorcy, która pozwala na odzyskanie komunikatu. Ta liczba d zostaje wybrana tak, aby iloczyn de zostawiał resztę 1 przy podzieleniu go przez $\phi(n)$. Ponieważ $n = pq$ jest iloczynem dwóch różnych liczb pierwszych, wartość $\phi(n) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1)$. Okazuje się, że istnieje zawsze tylko jedna liczba d w zakresie do $\phi(n)$ mająca wymaganą cechę.

Komputer Alicji może znaleźć d, wykorzystując algebraiczne narzędzie mające ponad 2300 lat, algorytm Euklidesa, który zaraz przeanalizujemy. Komputer Ewy mógłby oczywiście zrobić to samo, gdyby wiedział, jakie równanie ma rozwiązać. Jednak ponieważ p i q są tajemnicą Alicji, podobnie ma się rzecz z $(p - 1)(q - 1)$ i Ewa nie wie, od czego zacząć.

Istnienie d jest pewne tylko wtedy, gdy nadamy pewne łagodne ograniczenie na (znaną publicznie) szyfrująca liczbę e. Alicja musi sprawić, aby e nie miało wspólnego dzielnika pierwszego z $\phi(n)$. Dość łatwo spełnić ten warunek, gdyż Alicja może przetestować $\phi(n)$ pod kątem podzielności przez określone liczby pierwsze i sprawić, że e spełnia te wymagania, bez ujawniania wielkości p i q. W istocie wartością e często używaną w praktyce jest czwarta tak zwana *liczba pierwsza Fermata*, $e = 65537 = 2^{16} + 1$. Ta wartość, $2^{2^4} + 1$, ma szczególnie rzadką cechę: można zbudować regularny wielokąt o bokach e za pomocą linijki i cyrkla. Jej wykorzystanie w kryptografii wynika jednak z tego, że jest dość dużą liczbą pierwszą, która przekracza potęgę 2 dokładnie o 1, co prowadzi do wspomnianego wcześniej procesu szybkiego potęgowania.

Wróćmy do algorytmu Euklidesa. Rozpoczyna się on od obserwacji, że można znaleźć *największy wspólny dzielnik* (NWD) dwóch liczb $a > b$ przez kolejne odejmowania. Odnotujmy, że $r = a - b$ ma tę cechę, iż każdy wspólny dzielnik każdej z dwóch z trzech liczb a, b i r będzie także dzielnikiem trzeciej. Jeśli na przykład c jest wspólnym dzielnikiem a i b, czyli $a = ca_1$ oraz $b = cb_1$, wtedy $r = a - b = ca_1 - cb_1 = c(a_1 - b_1)$, co daje rozkład na czynniki r obejmujący dzielnik c. W szczególności NWD a i b jest taki sam jak b i r. Ponieważ obie te liczby są mniejsze od a, mamy teraz taki sam problem, ale w zastosowaniu do mniejszej pary liczb. Powtarzanie tego postępowania doprowadzi do pary, w której NWD jest oczywisty. (Istotnie dwie rozpatrywane liczby będą takie same, gdyż inaczej moglibyśmy wykonać jeszcze jeden krok. Ich wspólna wartość to liczba, której szukamy). Na przykład aby znaleźć NWD $a = 558$ i $b = 396$, pierwsze odejmowanie da nam $r = 558 - 396 = 162$, więc nasza nowa para to 396 i 162. Ponieważ $396 - 162 = 234$, naszą trzecią parą staje się 234 i 162, a kontynuując, otrzymujemy pełną listę liczb w postaci:

$$(558, 396) \to (396, 162) \to (234, 162) \to (162, 72) \to (90, 72) \to \\ \to (72, 18) \to (54, 18) \to (36, 18) \to (18, 18),$$

a więc NWD 558 i 396 to 18.