ĐỊNH LÝ FERMAT NHỎ

V. Senderov, A. Spivak

Định lý Fermat nhỏ được đưa vào chương trình học của các lớp Toán hiện nay. Công thức của định lý này do nhà Toán học Pie Fermat (người Pháp, 1601-1665) đưa ra năm 1640, rất ngắn gọn:

Nếu p là số nguyên tố và a là một số nguyên thế thì $a^p - a$ chia hết cho p.

Bề ngoài có vẻ đơn giản, tuy nhiên định lý này lại có những ứng dụng vô cùng quan trọng.

Các trường hợp riêng.

1. $p = 2$. Xét hiệu $a^2 - a = a(a-1)$. Trong hai số tự nhiên liên tiếp a và $a-1$, thì phải có một số chẵn và một số lẻ nên tích của chúng phải là một số chẵn.

Ta biết rằng a^2 và a có cùng tính chẵn lẻ do đó hiệu của chúng phải là số chẵn. Như vậy ta có thêm một cách chứng minh đơn giản cho trường hợp này.

2. $p = 3$. Xét hiệu $a^3 - a = (a+1)a(a-1)$. Một số chia cho 3 thì có số dư là $0, 1$ hoặc 2. Do đó trong 3 số tự nhiên liên tiếp $a+1, a, a-1$ phải có một số chia hết cho 3, và tích của chúng cũng chia hết cho 3. Dễ thấy hệ quả là hiệu trên chia hết cho 6.

Bài tập

1. Chứng minh $a^3 + 5a$ chia hết cho 6 với mọi số tự nhiên a.

Xét hiệu $a^4 - a$. Với $a = 2, a = 3$ thì $2^4 - 2 = 14, 3^4 - 3 = 78$ không chia hết cho 4. Như vậy ta thấy rằng phát biểu của định lý sẽ không đúng trong trường hợp p là hợp số.

3. $p = 5$. Xét hiệu $a^5 - a = (a^2+1)(a+1)a(a-1)$. Với $a = 1$, hiệu trên bằng 0; $a = 2$ thì $2^5 - 2 = 30$; $a = 3$ thì $3^5 - 3 = 240$; $a = 4$ thì $4^5 - 5 = 1020$; $a = 5$ thì $5^5 - 5 = 3120$; $a = 6$ thì $6^5 - 6 = 7770$. Tất cả các hiệu trên đều chia hết cho 30.

Nhận thấy $a^5 - a$ chia hết cho 2 và 3. Ta chứng minh hiệu này cũng chia hết cho 5.

Số tự nhiên a chia cho 5 thì có số dư k là $0, 1, 2, 3, 4$. Trường hợp số dư là $0, 1, 4$ thì từ sự phân tích ra thừa số ta suy ra hiệu $a^5 - a$ chia hết cho 5. Trường hợp số dư $k = 2$ thì

$$a^2+1=(5k+2)^2+1=5(5k^2+4k+1) \text{ chia hết cho } 5.$$

Tương tự với $k=3$. Vậy ta thu được điều phải chứng minh.

Ta có thể phân tích $a^2+1=(a-2)(a+2)+5$ và do đó

$$a^5-a=(a+2)(a+1)a(a-1)(a-2)+5(a+1)a(a-1)$$

có cùng số dư với $(a+2)(a+1)a(a-1)(a-2)$ khi chia cho 5.

Tích 5 số tự nhiên liên tiếp $(a+2)(a+1)a(a-1)(a-2)$ chia hết cho 5, do đó hiệu a^5-a cũng chia hết cho 5. Cũng nhận được hệ quả là hiệu này chia hết cho 30.

Vào năm 1801 K. F. Gauss đưa ra kí hiệu *đồng dư*. Ta sử dụng chúng để đơn giản hoá diễn đạt sự chia hết.

Hai số nguyên a,b gọi là đồng dư modulo n nếu chúng có cùng số dư khi chia cho số nguyên n. Kí hiệu là $a\equiv b\,(\mathrm{mod}\,n)$.

Giả sử $a\equiv b\,(\mathrm{mod}\,n)$, $c\equiv d\,(\mathrm{mod}\,n)$, dễ dàng chứng minh:

i. $a+c\equiv b+d\,(\mathrm{mod}\,n)$
ii. $ac\equiv bd\,(\mathrm{mod}\,n)$
iii. $a^m\equiv b^m\,(\mathrm{mod}\,n)$.

với a, b, n nguyên và m không âm.

Bài tập

2. Giải phương trình đồng dư $3x\equiv 11(\mathrm{mod}101)$.

3. Giải phương trình đồng dư $14x\equiv 0\,(\mathrm{mod}12)$.

4. Với $k\neq 0$. *Chứng minh rằng*

a. Nếu $ka\equiv kb\,(\mathrm{mod}\,kn)$ *thế thì* $a\equiv b\,(\mathrm{mod}\,n)$.

b. Nếu $ka\equiv kb\,(\mathrm{mod}\,n)$ *và* k *nguyên tố cùng nhau với* n *thế thì* $a\equiv b\,(\mathrm{mod}\,n)$.

4. $p=7$. Xét hiệu $a^7-a=(a-1)a(a+1)(a^2-a+1)(a^2+a+1)$.

Hãy thử một số giá trị của a: $0^7-0=0$, $1^7-1=0$, $2^7-2=126=7.18$, $6^7-7=279930=7.39990$.

Bây giờ ta sẽ chứng minh hiệu trên chia hết cho 7 với mọi số tự nhiên a. Ta có:

$a^2+a+1\equiv a^2+a-6\equiv(a-2)(a+3)\ (\mathrm{mod}\,7)$ và $a^2-a+1\equiv a^2-a-6=(a+2)(a-3)\ (\mathrm{mod}\,7)$

Suy ra hiệu trên đồng dư với tích bảy số tự nhiên liên tiếp. Số tự nhiên a chia cho 7 có số dư là 0, 1, 2, 3, 4, 5, 6 nên tích $(a+3)(a+2)(a+1)a(a-1)(a-2)(a-3)$ chia hết cho 7.

Bài tập

5. a. Chứng minh rằng $a^7 \equiv a \pmod{42}$.

b. Chứng minh rằng $a^9 \equiv a \pmod{30}$.

5. $p=11$. Xét hiệu $a^{11}-a=(a-1)a(a+1)(a^4+a^3+a^2+a+1)(a^4-a^3+a^2-a+1)$

Ta có $(a-3)(a-4)(a-5)(a-9)=(a^2-7a+12)(a^2-14a+45)\equiv(a^2+4a+1)(a^2-3a+1)$

$=a^4+a^3-10a^2+a+1\equiv a^4+a^3+a^2+a+1 \pmod{11}$. Tương tự, bạn có thể chỉ ra:

$(a-2)(a-6)(a-7)(a-8)=a^4-a^3+a^2-a+1$.

Như vậy hiệu trên đồng dư với tích 11 số tự nhiên liên tiếp, và tích này chia hết cho 11.

Tiếp tục với $p=13$ hoặc những số nguyên tố lớn hơn bạn có thể đưa ra từng lời giải riêng biệt cho từng trường hợp. Tuy nhiên, đã đến lúc chúng ta tiếp cận với trường hợp tổng quát của định lý Fermat nhỏ đối với mọi số nguyên tố p.

Bài tập

6. Chứng minh rằng

a. Tích của 4 số nguyên liên tiếp thì chia hết cho 24.

b. Tích của 5 số nguyên liên tiếp thì chia hết cho 120.

c. a^5-5a^3+4a *chia hết cho 120 với mọi số nguyên* a.

7. Chứng minh rằng a^5 *và* a *có chữ số tận cùng giống nhau.*

8. Chứng minh rằng $m^5n=mn^5$ *chia hết cho 30 với bất kì số nguyên* m,n.

9. Nếu số k *không chia hết cho 2, 3, 5 thế thì* k^4-1 *chia hết cho 240.*

10. a. Chứng minh rằng $2222^{5555}+5555^{2222}$ *chia hết cho 7.*

b. Tìm dư số của phép chia $(13^{14}+15^{16})+18^{19^{20}}$ *cho 7.*

11. Chứng minh tận cùng của $11^{10}-1$ *có hai chữ số tận cùng là hai số 0.*

12. a. Tìm tất cả các số nguyên a *sao cho* $a^{10}+1$ *có tận cùng là số 0.*

b. Chứng minh rằng $a^{100}+1$ *không thể tận cùng là số không với bất kì số nguyên* a *nào.*

13. Cho trước số chẵn n *khác không. Tìm ước chung lớn nhất của các số có dạng* a^n-a*, với* a *thuộc tập số nguyên.*

14. Cho trước số tự nhiên $n>1$*. Chứng minh rằng ước chung lớn nhất của các số dạng* a^n-a*,* a *thuộc tập số nguyên trùng với ước chung lớn nhất của các số dạng* a^n-a*, với* $a=1,2,3,...,2^n$.

Trường hợp tổng quát.

Xét số nguyên tố p và số nguyên k không chia hết cho p. Với $p=19$, $k=4$. Lập bảng xét các số $r=1,2,...,18$ và các dư số của $4r$ khi chia cho 19.

r	1	2	3	4	5	6	7	8	9
$4r$	4	8	12	16	20	24	28	32	36
$4r \bmod 19$	4	8	12	16	1	5	9	13	17
r	10	11	12	13	14	15	16	17	18
$4r$	40	44	48	52	56	60	64	68	72
$4r \bmod 19$	2	6	10	14	18	3	7	11	15

Ta nhận thấy rằng các số dư của $4r$ khi chia cho 19 đều đôi một khác nhau và chính là các số r. Tổng quát hơn ta có khẳng định

Nếu số nguyên k *không chia hết cho số nguyên tố* p *và* r_1, r_2 *là hai số dư phân biệt trong phép chia* k *cho* p *thì* kr_1, kr_2 *có hai số dư phân biệt khi chia cho* p.

Thật vậy nếu $kr_1-kr_2=k(r_1-r_2)\equiv 0 \pmod p$ thì do k không chia hết cho p, hay nói cách khác nguyên tố cùng nhau với p nên $r_1\equiv r_2 \pmod p$ hay $r_1=r_2$.

Bài tập

15. Tồn tại hay không số tự nhiên n *sao cho* $1999n$ *có tận cùng là 987654321?*

16. Nếu số nguyên k *nguyên tố cùng nhau với số tự nhiên* n *thì tồn tại số tự nhiên* x *sao cho* $kx-1$ *chia hết cho* n.

17. Nếu a,b *nguyên tố cùng nhau, thì bất kì số nguyên nào cũng có thể biểu diễn dưới dạng* $c=ax+by$*, với* x, y *nguyên.*

Bây giờ ta bàn đến lời giải của định lý Fermat nhỏ. Ta có thể viết $k^p-k=k(k^{p-1}-1)$. Như vậy nếu k chia hết cho p thì định lý là hiển nhiên nên quan trọng là trường hợp k không chia hết cho p.

Định lý 1.

Nếu số nguyên k không chia hết cho số nguyên tố p thì k^{p-1} có số dư là 1 khi chia cho p.

Chứng minh

Các số dư của các số $k, 2k, 3k, ..., (p-1)k$ đôi một khác nhau, và đó là $1, 2, 3, ..., p-1$. Như vậy

$$k.2k.3k...(p-1)k \equiv 1.2.3...(p-1) \pmod{p}$$

Hay $k^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$, suy ra $k^{p-1} \equiv 1 \pmod{p}$ (*).

Ở đây chúng ta sử dụng kết quả ở *Bài tập 4*. Có thể biến đổi $(k^{p-1}-1)(p-1)! \equiv 0 \pmod{p}$ và do $(p-1)!$ nguyên tố cùng nhau với p nên dẫn đến (*).

Bài tập

18. Tìm phần dư khi chia 3^{2000} *cho* 43.

19. Nếu số nguyên a *không chia hết cho 17, thế thì* $a^8 - 1$ *hoặc* $a^8 + 1$ *chia hết cho 17.*

20. Chứng minh rằng $m^{61}n - mn^{61}$ *chia hết cho 56786730 với mọi số nguyên* m, n.

21. Tìm tất cả các số nguyên tố p *sao cho* $5^{p^2} + 1$ *chia hết cho* p.

22. Chứng minh rằng $7^p - 5^p - 2$ *chia hết cho* $6p$ *với mọi số nguyên tố* p *lẻ.*

23. Với p *là số nguyên tố thế thì tổng* $1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1}$ *chia cho* p *dư* $p-1$.

24. Một số có 6 chữ số chia hết cho 7. Ta đổi chỗ chữ số hàng trăm nghìn lui về sau về hàng đơn vị. Chứng minh rằng số mới nhận được cũng chia hết cho 7. Thí dụ, 632387 *và* 200004 *chia hết cho 7 sau khi biến đổi nhận được 323876 và 42 cũng chia hết cho 7.*

25. Xét số nguyên tố p *khác 2, 3, 5. Chứng rằng số được lập bởi* $p-1$ *số 1 sẽ chia hết cho* p. *Thí dụ,* 111111 *chia hết cho 7.*

26. Chứng minh rằng với bất kì số nguyên tố* p *thì số* $9p$ *chữ số* $11...1122...22...99...99$ *(trong đó có* p *chữ số 1,* p *chữ số 2, ...,* p *chữ số 9) đồng dư với số 123456789 khi chia cho* p.

Các bảng nhân modulo.

Hãy xem xét $n-1$ số dư khác không trong phép chia một số cho n. Lập các bảng mà ô của hàng thứ a và cột thứ b là số dư của phép chia của tích ab cho n, trong đó $0 < a, b < n$.

Thí dụ với $n=5$ ta có *Bảng 1*, $n=11$ ta có *Bảng 2*.

×	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Bảng 1.

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Bảng 2.

×	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Bảng 3.

×	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

Bảng 4.

×	1	3
1	1	3
3	3	1

Bảng 5.

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Bảng 6.

Ta thấy rằng trong các bảng này số dư trong các ô cũng khác không. Đối với n là các số nguyên tố thì số dư tích hai số dư khác không cũng có số dư khác không trong phép chia cho n.

Đối với các hợp số n thì tích hai số dư của nó có thể có dư bằng 0 trong phép chia cho n. Thí dụ $2.2 \equiv 0 \pmod 4$ (xem *Bảng 3.*), và đối với $n=12$ thì xảy ra nhiều trường hợp hơn nữa (xem *Bảng 4.*) Bây giờ từ các bảng đã có xoá đi các cột và hàng có chứa số dư bằng 0. Thí dụ ở *Bảng 2* ta xoá đi hàng

thứ 2 và cột thứ 2 thì thu được bảng 5, ở *Bảng 4* xoá đi các cột và hàng thứ 2, 6, 8, 9, 10 thì thu được *Bảng 6*. Ở các bảng mà n là số nguyên tố thì không cần phải xoá đi hàng hay cột nào cả.

Nhận thấy rằng các hàng và cột được lại là những hàng và cột có số được đánh là nguyên tố cùng nhau với n. Ta có khẳng định (hãy chứng minh)

Hai số nguyên tố cùng nhau với n thì tích của chúng sẽ có số dư khác không modulo n.

Bài tập

27. Làm sáng tỏ tính đối xứng của các cặp số dư qua các đường chéo ở các bảng 1-6.

Định lý Euler.

Bây giờ ta sẽ có một sự tổng quát của định lý Fermat nhỏ cho trường hợp phép chia đối với một số tự nhiên n bất kì. Ta đã xem xét các bảng nhân modulo ở phần trước và nhận thấy rằng ô của hàng và cột được đánh số là nguyên tố cùng nhau với n thì sẽ có dư số khác không molulo n. Hơn nữa ở trong mỗi hàng hoặc mỗi cột trong các bảng mới nhận được đều có chứa số dư đôi một khác nhau modulo n. Có thể khẳng định nếu các số dư $a_1, a_2, a_3, ..., a_r$ modulo n đôi một khác nhau và nguyên tố cùng nhau với n thì các số $ka_1, ka_2, ..., ka_r$ có số dư cũng chính là các số $a_1, a_2, a_3, ..., a_r$ (hãy chứng minh). Ta có

$$ka_1.ka_2...ka_n \equiv a_1.a_2...a_n \pmod{n}$$

Từ đó $(k^r - 1)a_1a_2...a_n \equiv a_1a_2...a_n \pmod{n}$ do $a_1, a_2, ..., a_r$ đều nguyên tố cùng nhau với n nên $k^r \equiv 1 \pmod{n}$. Nếu n là số nguyên tố thì $r = n-1$, ta thu được khẳng định của định lý Fermat nhỏ. Khẳng định tổng quát được mang tên *Định lý Euler*.

Định lý 2.

Nếu số nguyên k nguyên tố cùng nhau với số tự nhiên n thì $k^r - 1$ chia hết cho n, với r là số các số tự nhiên nguyên tố cùng nhau với n mà không vượt quá n.

Bài tập

28. Chứng minh rằng nếu k chia hết cho 3, thế thì

a. k^3 chia cho 9 có dư số là 1 hoặc 8.

b. k^{81} chia cho 243 có dư số là 1 hoặc 242.

29. Chứng minh rằng

a. Nếu $a^3 + b^3 + c^3$ chia hết cho 9, thế thì một trong các số a, b, c chia hết cho 3.

b. Tổng các bình phương của 3 số nguyên chia hết cho 7 khi và chỉ khi tổng các luỹ thừa bậc 4 của những số nguyên đó chia hết cho 7.

30. Chứng minh rằng $7^{7^{7^{7}}} - 7^{7^{7}}$ *chia hết cho 10.*

31. Tìm 3 chữ số cuối cùng của 7^{9999}.

32. Nếu số nguyên a *nguyên tố cùng nhau với số tự nhiên* $n > 1$, *chứng minh rằng phương trình đồng dư* $ax \equiv b \pmod{n}$ *tương đương với* $x \equiv a^{r-1}b \pmod{n}$. *Trong đó* r *là số các số tự nhiên không bé hơn* n *nguyên tố cùng nhau với* n.

33. Chứng minh rằng nếu n *là số tự nhiên lẻ thế thì* $2^{n!} - 1$ *chia hết cho* n.

34. Tìm tất cả các số tự nhiên* $n > 1$ *sao cho tổng* $1^n + 2^n + ... + (n-1)^n$ *chia hết cho* n.

35. Chứng minh rằng với mỗi số tự nhiên* s *thì tồn tại một bội số* n *của nó sao cho tổng các chữ số của* n *chia hết cho* s.

Hàm Euler.

Năm 1763, Leonard Euler (1707-1783) đưa ra kí hiệu $\varphi(n)$ để chỉ số lượng các số dư modulo n mà nguyên tố cùng nhau với n. Thí dụ : $\varphi(1) = 1$, $\varphi(4) = 2$, $\varphi(12) = 4$.

Nếu p là số nguyên tố thế thì $\varphi(p) = p - 1$. Hãy xét $\varphi(p^m)$ với m là số tự nhiên. Các số dư modulo p^m là $0, 1, 2, ..., p^m - 1$. Trong đó có p^{m-1} số chia hết cho p là $0, p, 2p, ..., p^m - p$. Suy ra :

$$\varphi(p^m) = p^m - p^{m-1} = p^m(1 - \frac{1}{p})$$

Bây giờ thử tính $\varphi(1000)$, đó là số tất cả các số tự nhiên bé hơn 1000 và không chia hết cho 2 và 5. Có 500 số chẵn trong số các số tự nhiên bé hơn 1000. Có 200 số chia hết cho 5 trong số các số tự nhiên bé hơn 1000. Có 100 số chia hết cho 2 và 5 trong số các số tự nhiên bé hơn 1000. Như vậy thu được :

$$\varphi(1000) = 1000 - (500 + 200 - 100) = 400.$$

Bài tập

36. Tính $\varphi(2^a 5^b)$ *với* a *và* b *là các số tự nhiên.*

37. Với p, q *là hai số nguyên tố khác nhau. Tính* $\varphi(pq)$ *và* $\varphi(p^a q^b)$ *với* a, b *là các số tự nhiên.*

38. Giải phương trình :

a. $\varphi(7^x) = 294$

b. $\varphi(3^x 5^y) = 360$.

Áp dụng phương pháp tương tự ta có thể tính $\varphi(n)$ với mọi số nguyên dương n. Một thí dụ phức tạp hơn để làm rõ hơn phương pháp này, hãy tính $\varphi(300)$. Các số tự nhiên bé hơn 300 có 150 số chẵn, 100 số chia hết cho 3, 60 số chia hết cho 5. Trong số những bội này lại có 50 số chia hết cho 2.3=6, 30 số chia hết cho 2.5=10 và 20 số chia hết cho 3.5=15. Trong số các bội của 6, 10 và 15 này lại có 10 số chia hết cho 2.3.5=30. Như vậy ta có :

$$\varphi(300) = 300 - [150 + 100 + 60 - (50 + 30 + 20 - 10)] = 80$$

Để có phép chứng minh tổng quát sử dụng phương pháp này bạn có thể đọc bài báo « *Số học và những nguyên lý đếm* » của *N. Basileva* và *V. Gytenmakhera* đăng trong số *Kvant No2, năm 1994*. Và dưới đây là một cách chứng minh khác.

Định lý 3.

Hàm Euler có tính chất nhân, tức là $\varphi(mn) = \varphi(m)\varphi(n)$ *với* m, n *nguyên tố cùng nhau.*

Hệ quả.

Nếu n *có dạng phân tích chính tắc* $n = p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$ *với* $p_1, p_2, ..., p_s$ *là các ước nguyên tố phân biệt của* n *và* $a_1, a_2, ..., a_s$ *là các số tự nhiên. Thế thì*

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})....\varphi(p_s^{a_s}) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1})...(p_s^{a_s} - p_s^{a_s-1})$$

Chứng minh Định lý 3

Xét các số có dạng $mx + ny$ với $0 \le x < n$, $0 \le y < m$. Viết chúng thành một bảng $m \times n$ ô. Thí dụ với $n = 5, m = 8$, ta có bảng sau :

x \ y	0	1	2	3	4	5	6	7
0	0	5	10	15	20	25	30	35
1	8	13	18	23	28	33	38	43
2	16	21	26	31	36	41	46	51
3	24	29	34	39	44	49	54	59
4	32	37	42	47	52	57	62	67

Các số trong bảng trên phải có dư số đôi một khác nhau khi chia cho mn. Thật vậy nếu có

$$mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{mn}.$$

với $0 \le x_1, x_2 < n, 0 \le y_1, y_2 < m$. Thế thì ta có :

$$mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{n} \ (1) \text{ và } mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{m} \ (2)$$

Từ (1) suy ra $ny_1 \equiv ny_2 \pmod{m}$. Do m, n nguyên tố cùng nhau nên $y_1 \equiv y_2 \pmod{m}$. Hơn nữa $y_1, y_2 < m$ nên $y_1 = y_2$. Tương tự với (2) ta có $x_1 = x_2$.

Như vậy các số ở trên có số dư đôi một khác nhau khi chia cho mn. Hơn nữa tập các số dư này chính là tập $0,1,2,\ldots,mn-1$. Nói cách khác với mọi $d = 0,1,\ldots,mn-1$ đều tồn tại cặp số x, y sao cho $0 \le x < n,\ 0 \le y < m$ và $d \equiv mx + ny \pmod{mn}$.

Ta có $UCLN(mx+ny, m) = UCLN(ny, m) = UCLN(y, m)$. Tương tự $UCLN(mx+ny, n) = UCLN(x, n)$.

Có nghĩa là những số trong bảng trên nguyên tố cùng nhau với m sẽ nằm ở cột mà y nguyên tố cùng nhau với m, và những số nguyên tố cùng nhau với n sẽ nằm ở dòng mà x nguyên tố cùng nhau với n. Các số nguyên tố cùng nhau với mn sẽ là giao của các dòng và các cột đó.

Điều này chứng tỏ hệ thức $\varphi(m)\varphi(n) = \varphi(mn)$.

Bài tập

39. Viết các số từ 0 đến $mn-1$ vào bảng sau

0	1	2	…	$n-1$
n	$n+1$	$n+2$	…	$2n-1$
$2n$	$2n+1$	$2n+2$	…	$3n-1$
…	…	…	…	…
$(m-1)n$	$(m-1)n+1$	$(m-1)n+2$	…	$mn-1$

Chứng minh định lý Euler thông qua những mệnh đề sau

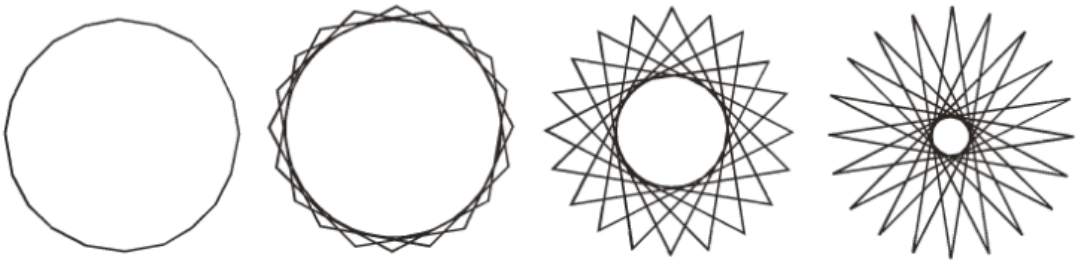
i. Những số nguyên tố cùng nhau với n lấp đầy $\varphi(n)$ cột của bảng trên.

ii. m số từ một cột bất kì của bảng trên có dư số đôi một khác nhau khi chia cho m.

iii. Từ mỗi cột có $\varphi(m)$ số nguyên tố cùng nhau với m.

iv. Một số nguyên tố cùng nhau với mn khi và chỉ khi số đó nguyên tố cùng nhau với m và n

40. Một đường tròn được phân chia thành n phần bằng nhau bởi n điểm. Có bao nhiêu đường gấp khúc kín mà các đoạn của nó đều bằng nhau và lấy các đỉnh thuộc vào tập n điểm trên.



Quy ước hai đường gấp khúc được coi là trùng nhau nếu đường này sẽ đồng nhất với đường kia qua một phép quay.

41. Chứng minh rằng với bất kì số tự nhiên m, n thì

a. $\varphi(m)\varphi(n) = \varphi(BCNN[m,n])\varphi(UCLN(m,n))$
b. $\varphi(mn) = \varphi(BCNN[m,n])UCLN(m,n)$
c. $\varphi(m)\varphi(n)UCLN(m,n) = \varphi(mn)\varphi(UCLN(m,n))$.

42. Giải các phương trình

a. $\varphi(x) = 18$.
b. $\varphi(x) = 12$.
c. $x - \varphi(x) = 12$.
d. $\varphi(x^2) = x^2 - x$.
e. $\varphi(x) = \frac{x}{2}$.
f. $\varphi(x) = \frac{x}{3}$.
g.* $\varphi(x) = \frac{x}{n}, n > 3$ *và là số tự nhiên.*
h. $\varphi(nx) = \varphi(x)$ *với số tự nhiên* $n > 1$.

Mật mã với chìa khoá mở.

Hãy tưởng tưởng rằng bạn nhận được một thông điệp mã hoá từ một người bạn, nhưng anh ta đã không thể gặp bạn trước đó, vậy loại mã hoá gì có thể sử dụng được trong trường hợp này. Có tồn tại phương pháp mã hoá nào mà có thể truyền tin khắp thế giới, thậm chí cả người bạn lẫn kẻ thù đều nhận được nhưng kẻ thù hoàn toàn không thể giải mã được thông điệp của bạn ?

Đó thật sự là một loại mã hoá tuyệt vời, nó khác hoàn toàn với các loại mã hoá thường sử dụng bí mật chủ yếu là chìa khoá, khi nắm mà được chìa khoá thì có thể mã hoá hay giải mã thông tin dễ dàng. Loại mật mã mới đề cập tới gọi là « Mật mã với chìa khoá mở », khi mà đã mã hoá thông điệp thì chỉ có tác giả mới có thể giải mã thông tin nhận được.

Mật mã RSA.

Năm 1978, ba nhà Toán học Rivest, Shamir và Adleman đã mã hoá một câu Anh ngữ và hứa sẽ trao giải 100 USD cho ai giải mã được thông điệp đó :

$y = 968696137546220614771409222543558829057599911245743198746951209308162$
$98225145708356931476622883989628013391990551829945157815154.$

Họ giải thích chi tiết phương pháp mã hoá. Các chữ cái được quy ước $a = 01, b = 02, ..., z = 26$ và dấu cách là 00. Sau đó họ viết câu thông thông điệp nhờ các chữ số trên thay thế cho các chữ cái được sắp liên tục thành một số x có 78 chữ số. Tiếp theo họ sử dụng một số nguyên tố p có 64 chữ số, một số nguyên tố q có 65 chữ số . Và tích của chúng là :

$pq = 114381625757888867669325779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541.$

Và họ chọn số y là dạng mã hoá của thông điệp nhờ công thức :

$$y \equiv x^{9007} \pmod{pq}$$

Họ công bố tích pq, số y và số nguyên tố 9007 và chính phương pháp mã hoá và cho biết số nguyên tố p có 64 chữ số, số nguyên tố q có 65 chữ số và x có 78 chữ số. Bí mật chỉ nằm ở hai số p, q có giá trị bằng bao nhiêu. Điều đòi hỏi là tìm x thoả mãn phương trình đồng dư trên.

Câu chuyện trên kết thúc vào năm 1994, khi mà Atkins, Kpaft, Lenstra và Leilang giải mã được câu thông điệp đó. Và hai số nguyên tố họ tìm được là :

$p = 34905295108476509491478496199038981334177646384933878439908205 77$
$q = 32769132993266709549961988190834461413177642967992942539798288533$

Trong cuốn *"Mở đầu về Lý thuyết Mật mã"* xuất bản năm 1998 của các nhà Toán học này viết rằng : *« Kết quả kỳ diệu này (sự phân tích một số có 129 chữ số thành nhân tử) đạt được nhờ một thuật toán phân tích một số thành nhân tử, có tên gọi là phương pháp* ***Sàn bình phương****. Quá trình thực hiên tính toán là nhờ vào sự cộng tác của cả một đội ngũ đông đảo. Điều hành dự án là bốn tác giả của lời giải với sự chuẩn bị bước đầu về lý thuyết số khoảng 220 ngày cộng với sự tham gia của gần 600 người và khoảng 1600 máy tính liên kết với nhau qua Internet. »*

Đáng tiếc là việc đi sâu vào phương pháp phân tích của họ đã vượt quá khuôn khổ của bài viết. Ta chấp nhận bỏ qua phần này và tiếp tục bàn luận về ý tưởng hệ thống mật mã RSA (đó chính là các chữ cái đầu của các nhà Toán học phát minh ra loại mật mã này).

Ý tưởng này như sau :

Cho các số nguyên tố p, q, tính được $\varphi(pq) = (p-1)(q-1)$.

Giả sử

$$ef = 1 + k\varphi(pq)$$

Ở đó e, f, k là các số tự nhiên. Với bất kì số tự nhiên x nguyên tố cùng nhau với pq thì theo định lý Euler

$$x^{ef} = x(x^k)^{\varphi(pq)} \equiv x.1 = x \pmod{pq}$$

Trong thí dụ của chúng ta thì $e = 9007$, và f thoả mãn phương trình đồng dư $ef \equiv 1(\mathrm{mod}\,\varphi(pq))$. Ở đây số e được chọn sao cho phải nguyên tố cùng nhau với $(p-1)(q-1)$, có thể lấy $e=1$ hoặc $e=(p-1)(q-1)-1$ nhưng sẽ không hợp lý nếu muốn giữ bí mật. Khi đó f tồn tại do thuật toán Euclid. Do điều kiện $y \equiv x^e \pmod{pq}$ nên

$$y^f \equiv x^{ef} \equiv x \pmod{pq}$$

Như vậy số x cần tìm là phần dư của y^f cho pq.

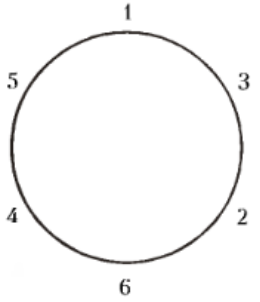
Tại sao mật mã RSA lại gọi là loại mật mã với chìa khoá mở ? Đó là tại vì số e và tích pq được người mã hoá thông điệp công khai. Khi mà mã hoá bất kì thông điệp nào thì chỉ cần có một máy tính cá nhân với một chương trình tính toán nào đó là đủ. Quá trình giải mã sẽ dễ dàng nếu biết được số f. Nhưng cách duy nhất để tính được f thì phải biết được giá trị của p và q, tức là cần phân tích pq thành nhân tử. Thuật toán phân tích một số thành thừa số nguyên tố là thuật toán có độ phức tạp mũ nên hi vọng có được lời giải là không có hiện thực. Ngay cả sự thành công năm 1994 của bốn nhà Toán học với phương pháp phân tích của họ chỉ có hiệu lực khi đã biết số chữ số của p và q, còn nếu không thì cả hệ thống liên kết của 600 con người và 1600 máy móc đó qua Internet đã phải đầu hàng.

Bài tập

43. (Dành cho các bạn yêu lập trình trên máy tính)*

a. *Tìm số f mà năm 1994 bốn nhà Toán học Atkins, Kpaft, Lenstra và Leilang đã tính toán được.*
b. *Giải mã câu Anh ngữ mà năm 1978 được mã hoá bởi Rivest, Shamir, Adleman.*

Một số bài toán đề nghị.



1. Chỉ ra sự tồn tại của các hợp số n sao cho với bất kì số nguyên a thì $a^n - a$ chia hết cho n (gọi là các số Carmichael)
2. Không tồn tại số tự nhiên n nào để $2^n + 1$ chia hết cho $n+1$.
3. Nếu $2^n + 1$ chia hết cho n thì $n=1$ hoặc $n=3$. Hãy chứng minh điều này.
4. Các điểm được đánh số $1, 2, \ldots, n-1$ có thể được xếp trên một đường tròn sao cho bất kì 3 số a, b, c liên tiếp nhau thì $b^2 - ac$ chia hết cho n. Tìm các số n như vậy. (Hình bên minh hoạ một trương hợp khi $n=7$)

5. Với những số nguyên tố p nào thì tồn tại số nguyên a sao cho $a^4+a^3+a^2+a+1$ chia hết cho p.

(Còn tiếp kì sau)