1. Пример работы алгоритма быстрого возведения в степень с модульной арифметикой:

13^{217} mod 57 = (13^{128} * 13^{64} * 13^{16} * 13^{8} * 13) mod 57 = <u>13</u>

Шаг	Основание степени	Результат
0	13	13 mod 57 = 13
1	13 mod 57	(13 * 13) mod 57 = 55 13^2 mod 57 = 55
2	13^2 mod 57	(55 * 55) mod 57 = 4 13^4 mod 57 = 4
3	13^4 mod 57	(4 * 4) mod 57 = 16 13^8 mod 57 = 16
4	13^8 mod 57	(16 * 16) mod 57 = 28 13^{16} mod 57 = 28
5	13^{16} mod 57	(28 * 28) mod 57 = 43 1332 mod 57 = 43
6	13^{32} mod 57	(43 * 43) mod 57 = 25 13^{64} mod 57 = 25
7	13^{64} mod 57	(25 *25) mod 57 = 55 13^{128} mod 57 = 55

13 mod 57 = 13
13^8 mod 57 = 16
13^{16} mod 57 = 28
13^{64} mod 57 = 25
13^{128} mod 57 = 55

(55 * 25 * 28 * 16 * 13) mod 57 = 13^{217} mod 57**;**
(55 * 25) mod 57 * (28 * 16) mod 57 * 13 mod 57 = (7 * 49) mod 57 * 13 mod 57 = (1 * 13) mod 57 = **13**

2. Пример поиска всех первообразных корней по заданному модулю

Простое число **p = 157**
Простые делители **p - 1 = phi = 156 ={2, 3, 13}**
Итерируем от **1** до **p – 1**
Если результат возведения в степень будет равен 1 по модулю p – значит порядок числа **g** меньше **p – 1** и он не является первообразным корнем:

$$g^{(phi / factor)} \bmod p != 1$$

Возможные степени:

156 / 2 = 78;
156 / 3 = 52;
156 / 13 = 12.

<u>g = 1:</u>

1^{78} mod 157 = 1
1^{52} mod 157 = 1

$1^{12} \bmod 157 = 1$

Не является первообразным корнем.

g = 2:

$2^{78} \bmod 157 = 156$

$2^{52} \bmod 157 = 1$

$2^{12} \bmod 157 = 14$

Не является первообразным корнем.

g = 3:

$3^{78} \bmod 157 = 1$

$3^{52} \bmod 157 = 113$

$3^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 4:

$4^{78} \bmod 157 = 1$

$4^{52} \bmod 157 = 64$

$4^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 5:

$5^{78} \bmod 157 = 156$

$5^{52} \bmod 157 = 25$

$5^{12} \bmod 157 = 125$

Является первообразным корнем.

g = 6:

$6^{78} \bmod 157 = 156$

$6^{52} \bmod 157 = 113$

$6^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 7:

$7^{78} \bmod 157 = 156$

$7^{52} \bmod 157 = 1$

$7^{12} \bmod 157 = 138$

Не является первообразным корнем.

g = 8:

$8^{78} \bmod 157 = 1$

$8^{52} \bmod 157 = 64$

$8^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 9:

$9^{78} \bmod 157 = 1$

$9^{52} \bmod 157 = 113$

$9^{12} \bmod 157 = 144$

Не является первообразным корнем ($9^{78} = 1$).

g = 10:

$10^{78} \bmod 157 = 1$

$10^{52} \bmod 157 = 25$

$10^{12} \bmod 157 = 125$

Не является первообразным корнем ($10^{78} = 1$).

g = 11:

$11^{78} \bmod 157 = 1$

$11^{52} \bmod 157 = 12$

$11^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 12:

$12^{78} \bmod 157 = 1$

$12^{52} \bmod 157 = 64$

$12^{12} \bmod 157 = 60$

Не является первообразным корнем ($12^{78} = 1$).

g = 13:

$13^{78} \bmod 157 = 1$

$13^{52} \bmod 157 = 58$

$13^{12} \bmod 157 = 129$

Не является первообразным корнем ($13^{78} = 1$).

g = 14:

$14^{78} \bmod 157 = 1$

$14^{52} \bmod 157 = 42$

$14^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 15:

$15^{78} \bmod 157 = 156$

$15^{52} \bmod 157 = 113$

$15^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 16:

$16^{78} \bmod 157 = 1$

$16^{52} \bmod 157 = 64$

$16^{12} \bmod 157 = 60$

Не является первообразным корнем ($16^{78} = 1$).

g = 17:

$17^{78} \bmod 157 = 1$

$17^{52} \bmod 157 = 153$

$17^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 18:

$18^{78} \bmod 157 = 156$

$18^{52} \bmod 157 = 113$

$18^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 19:

$19^{78} \bmod 157 = 1$

$19^{52} \bmod 157 = 58$

$19^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 20:

$20^{78} \bmod 157 = 156$

$20^{52} \bmod 157 = 25$

$20^{12} \bmod 157 = 125$

Является первообразным корнем.

g = 21:

$21^{78} \bmod 157 = 156$

$21^{52} \bmod 157 = 113$

$21^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 22:

$22^{78} \bmod 157 = 1$

$22^{52} \bmod 157 = 121$

$22^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 23:

$23^{78} \bmod 157 = 1$

$23^{52} \bmod 157 = 58$

$23^{12} \bmod 157 = 129$

Не является первообразным корнем ($23^{78}=1$).

g = 24:

$24^{78} \bmod 157 = 156$

$24^{52} \bmod 157 = 64$

$24^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 25:

$25^{78} \bmod 157 = 1$

$25^{52} \bmod 157 = 25$

$25^{12} \bmod 157 = 125$

Не является первообразным корнем ($25^{78}=1$).

g = 26:

$26^{78} \bmod 157 = 156$

$26^{52} \bmod 157 = 64$

$26^{12} \bmod 157 = 14$

Является первообразным корнем.

g = 27:

$27^{78} \bmod 157 = 1$

$27^{52} \bmod 157 = 113$

$27^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 28:

$28^{78} \bmod 157 = 1$

$28^{52} \bmod 157 = 42$

$28^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 29:

$29^{78} \bmod 157 = 1$

$29^{52} \bmod 157 = 153$

$29^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 30:

$30^{78} \bmod 157 = 1$

$30^{52} \bmod 157 = 113$

$30^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 31:

$31^{78} \bmod 157 = 1$

$31^{52} \bmod 157 = 25$

$31^{12} \bmod 157 = 125$

Не является первообразным корнем.

g = 32:

$32^{78} \bmod 157 = 1$

$32^{52} \bmod 157 = 64$

$32^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 33:

$33^{78} \bmod 157 = 1$

$33^{52} \bmod 157 = 113$

$33^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 34:

$34^{78} \bmod 157 = 156$

$34^{52} \bmod 157 = 64$

$34^{12} \bmod 157 = 14$

Является первообразным корнем.

g = 35:

$35^{78} \bmod 157 = 1$

$35^{52} \bmod 157 = 42$

$35^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 36:

$36^{78} \bmod 157 = 1$

$36^{52} \bmod 157 = 113$

$36^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 37:

$37^{78} \bmod 157 = 156$

$37^{52} \bmod 157 = 58$

$37^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 38:

$38^{78} \bmod 157 = 156$

$38^{52} \bmod 157 = 42$

$38^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 39:

$39^{78} \bmod 157 = 1$

$39^{52} \bmod 157 = 113$

$39^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 40:

$40^{78} \bmod 157 = 1$

$40^{52} \bmod 157 = 25$

$40^{12} \bmod 157 = 125$

Не является первообразным корнем.

g = 41:

$41^{78} \bmod 157 = 1$

$41^{52} \bmod 157 = 64$

$41^{12} \bmod 157 = 14$

Не является первообразным корнем.

g = 42:

$42^{78} \bmod 157 = 1$

$42^{52} \bmod 157 = 113$

$42^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 43:

$43^{78} \bmod 157 = 156$

$43^{52} \bmod 157 = 58$

$43^{12} \bmod 157 = 129$

Является первообразным корнем.

g = 44:

$44^{78} \bmod 157 = 1$

$44^{52} \bmod 157 = 42$

$44^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 45:

$45^{78} \bmod 157 = 1$

$45^{52} \bmod 157 = 113$

$45^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 46:

$46^{78} \bmod 157 = 1$

$46^{52} \bmod 157 = 153$

$46^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 47:

$47^{78} \bmod 157 = 1$

$47^{52} \bmod 157 = 58$

$47^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 48:

$48^{78} \bmod 157 = 1$

$48^{52} \bmod 157 = 64$

$48^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 49:

$49^{78} \bmod 157 = 1$

$49^{52} \bmod 157 = 25$

$49^{12} \bmod 157 = 125$

Не является первообразным корнем.

g = 50:

$50^{78} \bmod 157 = 1$

$50^{52} \bmod 157 = 64$

$50^{12} \bmod 157 = 14$

Не является первообразным корнем.

g = 51:

$51^{78} \bmod 157 = 1$

$51^{52} \bmod 157 = 113$

$51^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 52:

$52^{78} \bmod 157 = 1$

$52^{52} \bmod 157 = 64$

$52^{12} \bmod 157 = 14$

Не является первообразным корнем.

g = 53:

$53^{78} \bmod 157 = 156$

$53^{52} \bmod 157 = 153$

$53^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 54:

$54^{78} \bmod 157 = 1$

$54^{52} \bmod 157 = 113$

$54^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 55:

$55^{78} \bmod 157 = 156$

$55^{52} \bmod 157 = 25$

$55^{12} \bmod 157 = 125$

Является первообразным корнем.

g = 56:

$56^{78} \bmod 157 = 1$

$56^{52} \bmod 157 = 42$

$56^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 57:

$57^{78} \bmod 157 = 1$

$57^{52} \bmod 157 = 113$

$57^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 58:

$58^{78} \bmod 157 = 1$

$58^{52} \bmod 157 = 58$

$58^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 59:

$59^{78} \bmod 157 = 1$

$59^{52} \bmod 157 = 153$

$59^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 60:

$60^{78} \bmod 157 = 156$

$60^{52} \bmod 157 = 42$

$60^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 61:

$61^{78} \bmod 157 = 156$

$61^{52} \bmod 157 = 58$

$61^{12} \bmod 157 = 129$

Является первообразным корнем.

g = 62:

$62^{78} \bmod 157 = 156$

$62^{52} \bmod 157 = 113$

$62^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 63:

$63^{78} \bmod 157 = 156$

$63^{52} \bmod 157 = 25$

$63^{12} \bmod 157 = 125$

Является первообразным корнем.

g = 64:

$64^{78} \bmod 157 = 1$

$64^{52} \bmod 157 = 64$

$64^{12} \bmod 157 = 14$

Не является первообразным корнем.

g = 65:

$65^{78} \bmod 157 = 1$

$65^{52} \bmod 157 = 153$

$65^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 66:

$66^{78} \bmod 157 = 156$

$66^{52} \bmod 157 = 113$

$66^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 67:

$67^{78} \bmod 157 = 1$

$67^{52} \bmod 157 = 58$

$67^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 68:

$68^{78} \bmod 157 = 1$

$68^{52} \bmod 157 = 42$

$68^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 69:

$69^{78} \bmod 157 = 156$

$69^{52} \bmod 157 = 113$

$69^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 70:

$70^{78} \bmod 157 = 156$

$70^{52} \bmod 157 = 153$

$70^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 71:

$71^{78} \bmod 157 = 1$

$71^{52} \bmod 157 = 58$

$71^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 72:

$72^{78} \bmod 157 = 1$

$72^{52} \bmod 157 = 64$

$72^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 73:

$73^{78} \bmod 157 = 156$

$73^{52} \bmod 157 = 113$

$73^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 74:

$74^{78} \bmod 157 = 156$

$74^{52} \bmod 157 = 42$

$74^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 75:

$75^{78} \bmod 157 = 1$

$75^{52} \bmod 157 = 25$

$75^{12} \bmod 157 = 125$

Не является первообразным корнем.

g = 76:

$76^{78} \bmod 157 = 1$

$76^{52} \bmod 157 = 153$

$76^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 77:

$77^{78} \bmod 157 = 156$

$77^{52} \bmod 157 = 58$

$77^{12} \bmod 157 = 129$

Является первообразным корнем.

g = 78:

$78^{78} \bmod 157 = 1$

$78^{52} \bmod 157 = 113$

$78^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 79:

$79^{78} \bmod 157 = 1$

$79^{52} \bmod 157 = 42$

$79^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 80:

$80^{78} \bmod 157 = 156$

$80^{52} \bmod 157 = 64$

$80^{12} \bmod 157 = 14$

Является первообразным корнем.

g = 81:

$81^{78} \bmod 157 = 1$

$81^{52} \bmod 157 = 113$

$81^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 82:

$82^{78} \bmod 157 = 1$

$82^{52} \bmod 157 = 153$

$82^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 83:

$83^{78} \bmod 157 = 156$

$83^{52} \bmod 157 = 58$

$83^{12} \bmod 157 = 129$

Является первообразным корнем.

g = 84:

$84^{78} \bmod 157 = 156$

$84^{52} \bmod 157 = 42$

$84^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 85:

$85^{78} \bmod 157 = 156$

$85^{52} \bmod 157 = 113$

$85^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 86:

$86^{78} \bmod 157 = 1$

$86^{52} \bmod 157 = 153$

$86^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 87:

$87^{78} \bmod 157 = 156$

$87^{52} \bmod 157 = 58$

$87^{12} \bmod 157 = 129$

Является первообразным корнем.

g = 88:

$88^{78} \bmod 157 = 156$

$88^{52} \bmod 157 = 64$

$88^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 89:

$89^{78} \bmod 157 = 1$

$89^{52} \bmod 157 = 113$

$89^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 90:

$90^{78} \bmod 157 = 1$

$90^{52} \bmod 157 = 42$

$90^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 91:

$91^{78} \bmod 157 = 156$

$91^{52} \bmod 157 = 153$

$91^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 92:

$92^{78} \bmod 157 = 1$

$92^{52} \bmod 157 = 58$

$92^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 93:

$93^{78} \bmod 157 = 1$

$93^{52} \bmod 157 = 113$

$93^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 94:

$94^{78} \bmod 157 = 156$

$94^{52} \bmod 157 = 42$

$94^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 95:

$95^{78} \bmod 157 = 156$

$95^{52} \bmod 157 = 64$

$95^{12} \bmod 157 = 14$

Является первообразным корнем.

g = 96:

$96^{78} \bmod 157 = 156$

$96^{52} \bmod 157 = 113$

$96^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 97:

$97^{78} \bmod 157 = 156$

$97^{52} \bmod 157 = 153$

$97^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 98:

$98^{78} \bmod 157 = 1$

$98^{52} \bmod 157 = 58$

$98^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 99:

$99^{78} \bmod 157 = 1$

$99^{52} \bmod 157 = 42$

$99^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 100:

$100^{78} \bmod 157 = 1$

$100^{52} \bmod 157 = 25$

$100^{12} \bmod 157 = 125$

Не является первообразным корнем.

g = 101:

$101^{78} \bmod 157 = 1$

$101^{52} \bmod 157 = 153$

$101^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 102:

$102^{78} \bmod 157 = 156$

$102^{52} \bmod 157 = 113$

$102^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 103:

$103^{78} \bmod 157 = 1$

$103^{52} \bmod 157 = 58$

$103^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 104:

$104^{78} \bmod 157 = 156$

$104^{52} \bmod 157 = 42$

$104^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 105:

$105^{78} \bmod 157 = 1$

$105^{52} \bmod 157 = 25$

$105^{12} \bmod 157 = 125$

Не является первообразным корнем.

g = 106:

$106^{78} \bmod 157 = 1$

$106^{52} \bmod 157 = 64$

$106^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 107:

$107^{78} \bmod 157 = 1$

$107^{52} \bmod 157 = 113$

$107^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 108:

$108^{78} \bmod 157 = 1$

$108^{52} \bmod 157 = 42$

$108^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 109:

$109^{78} \bmod 157 = 1$

$109^{52} \bmod 157 = 153$

$109^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 110:

$110^{78} \bmod 157 = 1$

$110^{52} \bmod 157 = 58$

$110^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 111:

$111^{78} \bmod 157 = 1$

$111^{52} \bmod 157 = 113$

$111^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 112:

$112^{78} \bmod 157 = 1$

$112^{52} \bmod 157 = 42$

$112^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 113:

$113^{78} \bmod 157 = 1$

$113^{52} \bmod 157 = 113$

$113^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 114:

$114^{78} \bmod 157 = 156$

$114^{52} \bmod 157 = 153$

$114^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 115:

$115^{78} \bmod 157 = 1$

$115^{52} \bmod 157 = 58$

$115^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 116:

$116^{78} \bmod 157 = 1$

$116^{52} \bmod 157 = 42$

$116^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 117:

$117^{78} \bmod 157 = 1$

$117^{52} \bmod 157 = 113$

$117^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 118:

$118^{78} \bmod 157 = 1$

$118^{52} \bmod 157 = 153$

$118^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 119:

$119^{78} \bmod 157 = 156$

$119^{52} \bmod 157 = 58$

$119^{12} \bmod 157 = 129$

Является первообразным корнем.

g = 120:

$120^{78} \bmod 157 = 1$

$120^{52} \bmod 157 = 42$

$120^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 121:

$121^{78} \bmod 157 = 1$

$121^{52} \bmod 157 = 121$

$121^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 122:

$122^{78} \bmod 157 = 1$

$122^{52} \bmod 157 = 113$

$122^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 123:

$123^{78} \bmod 157 = 156$

$123^{52} \bmod 157 = 153$

$123^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 124:

$124^{78} \bmod 157 = 1$

$124^{52} \bmod 157 = 58$

$124^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 125:

$125^{78} \bmod 157 = 1$

$125^{52} \bmod 157 = 25$

$125^{12} \bmod 157 = 125$

Не является первообразным корнем.

g = 126:

$126^{78} \bmod 157 = 1$

$126^{52} \bmod 157 = 42$

$126^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 127:

$127^{78} \bmod 157 = 1$

$127^{52} \bmod 157 = 113$

$127^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 128:

$128^{78} \bmod 157 = 1$

$128^{52} \bmod 157 = 64$

$128^{12} \bmod 157 = 14$

Не является первообразным корнем.

g = 129:

$129^{78} \bmod 157 = 1$

$129^{52} \bmod 157 = 153$

$129^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 130:

$130^{78} \bmod 157 = 1$

$130^{52} \bmod 157 = 58$

$130^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 131:

$131^{78} \bmod 157 = 156$

$131^{52} \bmod 157 = 42$

$131^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 132:

$132^{78} \bmod 157 = 1$

$132^{52} \bmod 157 = 113$

$132^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 133:

$133^{78} \bmod 157 = 156$

$133^{52} \bmod 157 = 153$

$133^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 134:

$134^{78} \bmod 157 = 1$

$134^{52} \bmod 157 = 58$

$134^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 135:

$135^{78} \bmod 157 = 1$

$135^{52} \bmod 157 = 42$

$135^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 136:

$136^{78} \bmod 157 = 156$

$136^{52} \bmod 157 = 113$

$136^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 137:

$137^{78} \bmod 157 = 156$

$137^{52} \bmod 157 = 153$

$137^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 138:

$138^{78} \bmod 157 = 1$

$138^{52} \bmod 157 = 58$

$138^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 139:

$139^{78} \bmod 157 = 156$

$139^{52} \bmod 157 = 42$

$139^{12} \bmod 157 = 60$

Является первообразным корнем.

g = 140:

$140^{78} \bmod 157 = 1$

$140^{52} \bmod 157 = 113$

$140^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 141:

$141^{78} \bmod 157 = 1$

$141^{52} \bmod 157 = 153$

$141^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 142:

$142^{78} \bmod 157 = 156$

$142^{52} \bmod 157 = 58$

$142^{12} \bmod 157 = 129$

Является первообразным корнем.

g = 143:

$143^{78} \bmod 157 = 1$

$143^{52} \bmod 157 = 42$

$143^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 144:

$144^{78} \bmod 157 = 1$

$144^{52} \bmod 157 = 144$

$144^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 145:

$145^{78} \bmod 157 = 1$

$145^{52} \bmod 157 = 113$

$145^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 146:

$146^{78} \bmod 157 = 1$

$146^{52} \bmod 157 = 153$

$146^{12} \bmod 157 = 152$

Не является первообразным корнем.

g = 147:

$147^{78} \bmod 157 = 1$

$147^{52} \bmod 157 = 58$

$147^{12} \bmod 157 = 129$

Не является первообразным корнем.

g = 148:

$148^{78} \bmod 157 = 15$

$148^{52} \bmod 157 = 42$

$148^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 149:

$149^{78} \bmod 157 = 1$

$149^{52} \bmod 157 = 113$

$149^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 150:

$150^{78} \bmod 157 = 1$

$150^{52} \bmod 157 = 153$

$150^{12} \bmod 157 = 25$

Не является первообразным корнем.

g = 151:

$151^{78} \bmod 157 = 156$

$151^{52} \bmod 157 = 36$

$151^{12} \bmod 157 = 144$

Является первообразным корнем.

g = 152:

$152^{78} \bmod 157 = 156$

$152^{52} \bmod 157 = 153$

$152^{12} \bmod 157 = 152$

Является первообразным корнем.

g = 153:

$153^{78} \bmod 157 = 1$

$153^{52} \bmod 157 = 153$

$153^{12} \bmod 157 = 144$

Не является первообразным корнем.

g = 154:

$154^{78} \bmod 157 = 1$

$154^{52} \bmod 157 = 42$

$154^{12} \bmod 157 = 60$

Не является первообразным корнем.

g = 155:

$155^{78} \bmod 157 = 1$

$155^{52} \bmod 157 = 121$

$155^{12} \bmod 157 = 125$

Не является первообразным корнем.

g = 156:

$156^{78} \bmod 157 = 1$

$156^{52} \bmod 157 = 1$

$156^{12} \bmod 157 = 1$

Не является первообразным корнем.

Итоговый список первообразных корней (48 штук):

5 6 15 18 20 21 24 26 34 38 43 53 55 60 61 62 63 66 69 70 72 73 74 77 80 83 84 85 87 88 91 94 95 96 97 102 104 114 119 123 131 133 136 137 139 142 151 152

Количество: 48 (что соответствует $\varphi(156) = 48$).

3. Пример работы расширенного алгоритма Евклида с взаимно простыми числами

$x_1 * a + y_1 * b = НОД(a, b)$, $a = 59$, $b = 37$

Итерация	q	a_0	a_1	x_0	x_1	y_0	y_1
0	-	59	37	1	0	0	1
1	1	37	22	0	1	1	-1
2	1	22	15	1	-1	-1	2
3	1	15	7	-1	2	2	-3
4	2	7	1	2	-3	-3	8
5	7	1	0	**-3**	8	**8**	-59

$x_1 = -3$

$y_1 = 8$

$-3 * 59 + 8 * 37 = 1$