

# Criptografía y Seguridad - Tarea 2

Rivera González Damián  
Tadeo Guillén Diana G

October 29, 2019

## Ejercicio 1

Mostrar las siguientes propiedades del símbolo de Jacobi, partiendo de lo demostrado en clase del símbolo de Legendre

1. Si  $a \equiv b \pmod{n}$ , se tiene  $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

*Proof.* De acuerdo a la definición del símbolo de Jacobi, tenemos  $n = \prod_{i=1}^k P_i^{e_i}$  como la descomposición de primos de  $n$ . Por otro lado sabemos que  $a \equiv b \pmod{n}$  por lo que tenemos  $a \equiv b \pmod{P_i^{e_i}}$  para cada  $P_i^{e_i}$ .

También sabemos que si  $a \equiv b \pmod{p}$  entonces  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$  para algún primo  $p$ , en particular, para  $P_i^{e_i}$  se cumple también que si  $a \equiv b \pmod{P_i^{e_i}} \implies \left(\frac{a}{P_i^{e_i}}\right) = \left(\frac{b}{P_i^{e_i}}\right)$

Entonces tenemos que  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$  implica  $\prod_{i=1}^k \frac{a}{P_i^{e_i}} = \prod_{i=1}^k \frac{b}{P_i^{e_i}}$  y por lo tanto

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

□

2.  $\left(\frac{1}{p}\right) = 1$

*Proof.* De acuerdo al símbolo de Legendre  $(1, p) = 1$  pues para  $\left(\frac{a}{p}\right) = 1$  si y solo si  $(a, p) = 1$  y  $a$  es RC modulo  $p$ . En este caso, es fácil ver que  $(1, p) = 1$  para cualquier  $p$  y por el pequeño teorema de Fermat, sabemos que  $a^{p-1} \equiv 1 \pmod{p}$  para cualquier  $p$  y tomando nuestro caso particular  $a = 1$  obteniendo 1 como RC.

Como lo anterior se aplica para Jacobi también

$$(1, p) = 1$$

□

3.  $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

*Proof.* De acuerdo con el símbolo de Legendre, para  $p$  un primo impar, se tiene  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Sea el caso de  $n$  primo, por definición cumple. Por otro lado, suponemos a  $n = p_1 * p_2$

con  $p_1$  y  $p_2$  primos.

Entonces tenemos que  $\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)$  donde

$$\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right) = (-1)^{\frac{(p_1-1)}{2}}(-1)^{\frac{(p_2-1)}{2}} = (-1)^{(p_1-1)/2+(p_2-1)/2} = (-1)^{(p_1*p_2-1)/2}$$

que a su vez, de acuerdo a un lema de otra propiedad de Legendre, obtenemos

$$(-1)^{(p_1*p_2-1)/2} = (-1)^{\frac{n-1}{2}}$$

así que si procedemos a descomponer a  $n$  en primos tendríamos que  $\left(\frac{-1}{p}\right) = \prod_{i=1}^k \frac{-1}{P_i^{e_i}}$

que es lo mismo que  $\left(\frac{-1}{p}\right) = \prod_{i=1}^k [(-1)^{\frac{(p_i-1)}{2}}]^{e_i}$ .

Entonces obtenemos

$$\left(\frac{-1}{p}\right) = (-1)^{\sum_{i=1}^k e_i \frac{(p_i-1)}{2}} = (-1)^{\frac{(n-1)}{2}}$$

para  $k$  primos □

4.  $\left(\frac{ab...l}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)...\left(\frac{l}{n}\right)$

*Proof.* Sabemos que para el símbolo de Legendre se cumple la propiedad  $\left(\frac{ab...l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)...\left(\frac{l}{p}\right)$  para algún  $p$  primo, por lo que, si descomponemos a  $n$  en primos, tendremos:

$$\left(\frac{ab...l}{n}\right) = \prod_{i=1}^k \frac{ab...l}{P_i^{e_i}} = \prod_{i=1}^k \left(\frac{a}{P_i^{e_i}}\right) \left(\frac{b}{P_i^{e_i}}\right) \cdots \left(\frac{l}{P_i^{e_i}}\right)$$

para cada  $P_i$  primo. Esto implica que

$$\left(\frac{ab...l}{n}\right) = \prod_{i=1}^k \frac{a}{P_i^{e_i}} \prod_{i=1}^k \frac{b}{P_i^{e_i}} \cdots \prod_{i=1}^k \frac{l}{P_i^{e_i}} = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right) \cdots \left(\frac{l}{n}\right)$$

Por lo tanto

$$\left(\frac{ab...l}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right) \cdots \left(\frac{l}{n}\right)$$

□

5.  $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

*Proof.* Sabemos por Legendre que  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ . Si suponemos para  $n$  primo, entonces tenemos que por supuesto lo cumple, ahora veamos con  $n$  producto de 2 enteros donde  $n = p_1 * p_2$

En este caso tenemos que

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right) \left(\frac{2}{p_2}\right) = (-1)^{\frac{(p_1^2-1)}{8}} (-1)^{\frac{(p_2^2-1)}{8}}$$

Donde se obtiene

$$(-1)^{(p_1^2-1)/8} (-1)^{(p_2^2-1)/8} = (-1)^{((p_1*p_2)^2-1)/8} = (-1)^{(n^2-1)/8}$$

Por lo anterior podemos generalizarlo para descomponer  $n$  en varios primos de forma que  $\left(\frac{2}{n}\right) = \prod_{i=1}^k \frac{2}{P_i^{e_i}}$  Y por el resultado anterior

$$\left(\frac{2}{n}\right) = \prod_{i=1}^k (-1)^{e_i(P_i^2-1)/8} = (-1)^{\sum_{i=1}^k e_i(P_i^2-1)/8} = (-1)^{(n^2-1)/8}$$

□

6. Si se tienen  $p$  y  $q$  primos impares tales que  $(p, q) = 1$  se tiene que:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2} \frac{(q-1)}{2}} \left(\frac{p}{q}\right)$$

*Proof.* Por el símbolo de Legendre sabemos que

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)}{2} \frac{(q-1)}{2}}$$

y por lo tanto

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2} \frac{(q-1)}{2}} \left(\frac{p}{q}\right)$$

□

## Ejercicio 2

a) Muestra que 2 es generados de  $\mathbb{Z}_{2027}^*$

Veremos que se generan todos los valores de 1 a 2026:

$1 = 2^{2026} \text{mod}(2027)$	$22 = 2^{1312} \text{mod}(2027)$	$43 = 2^{489} \text{mod}(2027)$
$2 = 2^1 \text{mod}(2027)$	$23 = 2^{2007} \text{mod}(2027)$	$44 = 2^{1313} \text{mod}(2027)$
$3 = 2^{282} \text{mod}(2027)$	$24 = 2^{285} \text{mod}(2027)$	$45 = 2^{507} \text{mod}(2027)$
$4 = 2^2 \text{mod}(2027)$	$25 = 2^{1912} \text{mod}(2027)$	$46 = 2^{2008} \text{mod}(2027)$
$5 = 2^{1969} \text{mod}(2027)$	$26 = 2^{1885} \text{mod}(2027)$	$47 = 2^{807} \text{mod}(2027)$
$6 = 2^{283} \text{mod}(2027)$	$27 = 2^{846} \text{mod}(2027)$	$48 = 2^{286} \text{mod}(2027)$
$7 = 2^{1755} \text{mod}(2027)$	$28 = 2^{1757} \text{mod}(2027)$	$49 = 2^{1484} \text{mod}(2027)$
$8 = 2^3 \text{mod}(2027)$	$29 = 2^{609} \text{mod}(2027)$	$50 = 2^{1913} \text{mod}(2027)$
$9 = 2^{564} \text{mod}(2027)$	$30 = 2^{226} \text{mod}(2027)$	$51 = 2^{1938} \text{mod}(2027)$
$10 = 2^{1970} \text{mod}(2027)$	$31 = 2^{1496} \text{mod}(2027)$	$52 = 2^{1886} \text{mod}(2027)$
$11 = 2^{1311} \text{mod}(2027)$	$32 = 2^5 \text{mod}(2027)$	$53 = 2^{1832} \text{mod}(2027)$
$12 = 2^{284} \text{mod}(2027)$	$33 = 2^{1593} \text{mod}(2027)$	$54 = 2^{847} \text{mod}(2027)$
$13 = 2^{1884} \text{mod}(2027)$	$34 = 2^{1657} \text{mod}(2027)$	$55 = 2^{1254} \text{mod}(2027)$
$14 = 2^{1756} \text{mod}(2027)$	$35 = 2^{1698} \text{mod}(2027)$	$56 = 2^{1758} \text{mod}(2027)$
$15 = 2^{225} \text{mod}(2027)$	$36 = 2^{566} \text{mod}(2027)$	$57 = 2^{1346} \text{mod}(2027)$
$16 = 2^4 \text{mod}(2027)$	$37 = 2^{775} \text{mod}(2027)$	$58 = 2^{610} \text{mod}(2027)$
$17 = 2^{1656} \text{mod}(2027)$	$38 = 2^{1065} \text{mod}(2027)$	$59 = 2^{1393} \text{mod}(2027)$
$18 = 2^{565} \text{mod}(2027)$	$39 = 2^{140} \text{mod}(2027)$	$60 = 2^{227} \text{mod}(2027)$
$19 = 2^{1064} \text{mod}(2027)$	$40 = 2^{1972} \text{mod}(2027)$	$61 = 2^{1176} \text{mod}(2027)$
$20 = 2^{1971} \text{mod}(2027)$	$41 = 2^{94} \text{mod}(2027)$	$62 = 2^{1497} \text{mod}(2027)$
$21 = 2^{11} \text{mod}(2027)$	$42 = 2^{12} \text{mod}(2027)$	$63 = 2^{293} \text{mod}(2027)$

$64 = 2^6 \text{mod}(2027)$	$114 = 2^{1347} \text{mod}(2027)$	$164 = 2^{96} \text{mod}(2027)$
$65 = 2^{1827} \text{mod}(2027)$	$115 = 2^{1950} \text{mod}(2027)$	$165 = 2^{1536} \text{mod}(2027)$
$66 = 2^{1594} \text{mod}(2027)$	$116 = 2^{611} \text{mod}(2027)$	$166 = 2^{401} \text{mod}(2027)$
$67 = 2^{417} \text{mod}(2027)$	$117 = 2^{422} \text{mod}(2027)$	$167 = 2^{710} \text{mod}(2027)$
$68 = 2^{1658} \text{mod}(2027)$	$118 = 2^{1394} \text{mod}(2027)$	$168 = 2^{14} \text{mod}(2027)$
$69 = 2^{263} \text{mod}(2027)$	$119 = 2^{1385} \text{mod}(2027)$	$169 = 2^{1742} \text{mod}(2027)$
$70 = 2^{1699} \text{mod}(2027)$	$120 = 2^{228} \text{mod}(2027)$	$170 = 2^{1600} \text{mod}(2027)$
$71 = 2^{1422} \text{mod}(2027)$	$121 = 2^{596} \text{mod}(2027)$	$171 = 2^{1628} \text{mod}(2027)$
$72 = 2^{567} \text{mod}(2027)$	$122 = 2^{1177} \text{mod}(2027)$	$172 = 2^{491} \text{mod}(2027)$
$73 = 2^{1925} \text{mod}(2027)$	$123 = 2^{376} \text{mod}(2027)$	$173 = 2^{1200} \text{mod}(2027)$
$74 = 2^{776} \text{mod}(2027)$	$124 = 2^{1498} \text{mod}(2027)$	$174 = 2^{892} \text{mod}(2027)$
$75 = 2^{168} \text{mod}(2027)$	$125 = 2^{1855} \text{mod}(2027)$	$175 = 2^{1641} \text{mod}(2027)$
$76 = 2^{1066} \text{mod}(2027)$	$126 = 2^{294} \text{mod}(2027)$	$176 = 2^{1315} \text{mod}(2027)$
$77 = 2^{1040} \text{mod}(2027)$	$127 = 2^{1965} \text{mod}(2027)$	$177 = 2^{1675} \text{mod}(2027)$
$78 = 2^{141} \text{mod}(2027)$	$128 = 2^7 \text{mod}(2027)$	$178 = 2^{1991} \text{mod}(2027)$
$79 = 2^{987} \text{mod}(2027)$	$129 = 2^{771} \text{mod}(2027)$	$179 = 2^{312} \text{mod}(2027)$
$80 = 2^{1973} \text{mod}(2027)$	$130 = 2^{1828} \text{mod}(2027)$	$180 = 2^{509} \text{mod}(2027)$
$81 = 2^{1128} \text{mod}(2027)$	$131 = 2^{259} \text{mod}(2027)$	$181 = 2^{268} \text{mod}(2027)$
$82 = 2^{95} \text{mod}(2027)$	$132 = 2^{1595} \text{mod}(2027)$	$182 = 2^{1614} \text{mod}(2027)$
$83 = 2^{400} \text{mod}(2027)$	$133 = 2^{793} \text{mod}(2027)$	$183 = 2^{1458} \text{mod}(2027)$
$84 = 2^{13} \text{mod}(2027)$	$134 = 2^{418} \text{mod}(2027)$	$184 = 2^{2010} \text{mod}(2027)$
$85 = 2^{1599} \text{mod}(2027)$	$135 = 2^{789} \text{mod}(2027)$	$185 = 2^{718} \text{mod}(2027)$
$86 = 2^{490} \text{mod}(2027)$	$136 = 2^{1659} \text{mod}(2027)$	$186 = 2^{1779} \text{mod}(2027)$
$87 = 2^{891} \text{mod}(2027)$	$137 = 2^{1532} \text{mod}(2027)$	$187 = 2^{941} \text{mod}(2027)$
$88 = 2^{1314} \text{mod}(2027)$	$138 = 2^{264} \text{mod}(2027)$	$188 = 2^{809} \text{mod}(2027)$
$89 = 2^{1990} \text{mod}(2027)$	$139 = 2^{385} \text{mod}(2027)$	$189 = 2^{575} \text{mod}(2027)$
$90 = 2^{508} \text{mod}(2027)$	$140 = 2^{1700} \text{mod}(2027)$	$190 = 2^{1008} \text{mod}(2027)$
$91 = 2^{1613} \text{mod}(2027)$	$141 = 2^{1089} \text{mod}(2027)$	$191 = 2^{1491} \text{mod}(2027)$
$92 = 2^{2009} \text{mod}(2027)$	$142 = 2^{1423} \text{mod}(2027)$	$192 = 2^{288} \text{mod}(2027)$
$93 = 2^{1778} \text{mod}(2027)$	$143 = 2^{1169} \text{mod}(2027)$	$193 = 2^{1002} \text{mod}(2027)$
$94 = 2^{808} \text{mod}(2027)$	$144 = 2^{568} \text{mod}(2027)$	$194 = 2^{1960} \text{mod}(2027)$
$95 = 2^{1007} \text{mod}(2027)$	$145 = 2^{552} \text{mod}(2027)$	$195 = 2^{83} \text{mod}(2027)$
$96 = 2^{287} \text{mod}(2027)$	$146 = 2^{1926} \text{mod}(2027)$	$196 = 2^{1486} \text{mod}(2027)$
$97 = 2^{1959} \text{mod}(2027)$	$147 = 2^{1766} \text{mod}(2027)$	$197 = 2^{389} \text{mod}(2027)$
$98 = 2^{1485} \text{mod}(2027)$	$148 = 2^{777} \text{mod}(2027)$	$198 = 2^{1876} \text{mod}(2027)$
$99 = 2^{1875} \text{mod}(2027)$	$149 = 2^{1663} \text{mod}(2027)$	$199 = 2^{1844} \text{mod}(2027)$
$100 = 2^{1914} \text{mod}(2027)$	$150 = 2^{169} \text{mod}(2027)$	$200 = 2^{1915} \text{mod}(2027)$
$101 = 2^{797} \text{mod}(2027)$	$151 = 2^{1161} \text{mod}(2027)$	$201 = 2^{699} \text{mod}(2027)$
$102 = 2^{1939} \text{mod}(2027)$	$152 = 2^{1067} \text{mod}(2027)$	$202 = 2^{798} \text{mod}(2027)$
$103 = 2^{1648} \text{mod}(2027)$	$153 = 2^{194} \text{mod}(2027)$	$203 = 2^{338} \text{mod}(2027)$
$104 = 2^{1887} \text{mod}(2027)$	$154 = 2^{1041} \text{mod}(2027)$	$204 = 2^{1940} \text{mod}(2027)$
$105 = 2^{1980} \text{mod}(2027)$	$155 = 2^{1439} \text{mod}(2027)$	$205 = 2^{37} \text{mod}(2027)$
$106 = 2^{1833} \text{mod}(2027)$	$156 = 2^{142} \text{mod}(2027)$	$206 = 2^{1649} \text{mod}(2027)$
$107 = 2^{1245} \text{mod}(2027)$	$157 = 2^{1898} \text{mod}(2027)$	$207 = 2^{545} \text{mod}(2027)$
$108 = 2^{848} \text{mod}(2027)$	$158 = 2^{988} \text{mod}(2027)$	$208 = 2^{1888} \text{mod}(2027)$
$109 = 2^{249} \text{mod}(2027)$	$159 = 2^{88} \text{mod}(2027)$	$209 = 2^{349} \text{mod}(2027)$
$110 = 2^{1255} \text{mod}(2027)$	$160 = 2^{1974} \text{mod}(2027)$	$210 = 2^{1981} \text{mod}(2027)$
$111 = 2^{1057} \text{mod}(2027)$	$161 = 2^{1736} \text{mod}(2027)$	$211 = 2^{456} \text{mod}(2027)$
$112 = 2^{1759} \text{mod}(2027)$	$162 = 2^{1129} \text{mod}(2027)$	$212 = 2^{1834} \text{mod}(2027)$
$113 = 2^{1190} \text{mod}(2027)$	$163 = 2^{125} \text{mod}(2027)$	$213 = 2^{1704} \text{mod}(2027)$

$214 = 2^{1246} \bmod(2027)$	$264 = 2^{1596} \bmod(2027)$	$314 = 2^{1899} \bmod(2027)$
$215 = 2^{432} \bmod(2027)$	$265 = 2^{1775} \bmod(2027)$	$315 = 2^{236} \bmod(2027)$
$216 = 2^{849} \bmod(2027)$	$266 = 2^{794} \bmod(2027)$	$316 = 2^{989} \bmod(2027)$
$217 = 2^{1225} \bmod(2027)$	$267 = 2^{246} \bmod(2027)$	$317 = 2^{559} \bmod(2027)$
$218 = 2^{250} \bmod(2027)$	$268 = 2^{419} \bmod(2027)$	$318 = 2^{89} \bmod(2027)$
$219 = 2^{181} \bmod(2027)$	$269 = 2^{1852} \bmod(2027)$	$319 = 2^{1920} \bmod(2027)$
$220 = 2^{1256} \bmod(2027)$	$270 = 2^{790} \bmod(2027)$	$320 = 2^{1975} \bmod(2027)$
$221 = 2^{1514} \bmod(2027)$	$271 = 2^{1086} \bmod(2027)$	$321 = 2^{1527} \bmod(2027)$
$222 = 2^{1058} \bmod(2027)$	$272 = 2^{1660} \bmod(2027)$	$322 = 2^{1737} \bmod(2027)$
$223 = 2^{394} \bmod(2027)$	$273 = 2^{1895} \bmod(2027)$	$323 = 2^{694} \bmod(2027)$
$224 = 2^{1760} \bmod(2027)$	$274 = 2^{1533} \bmod(2027)$	$324 = 2^{1130} \bmod(2027)$
$225 = 2^{450} \bmod(2027)$	$275 = 2^{1197} \bmod(2027)$	$325 = 2^{1770} \bmod(2027)$
$226 = 2^{1191} \bmod(2027)$	$276 = 2^{265} \bmod(2027)$	$326 = 2^{126} \bmod(2027)$
$227 = 2^{1466} \bmod(2027)$	$277 = 2^{572} \bmod(2027)$	$327 = 2^{531} \bmod(2027)$
$228 = 2^{1348} \bmod(2027)$	$278 = 2^{386} \bmod(2027)$	$328 = 2^{97} \bmod(2027)$
$229 = 2^{1093} \bmod(2027)$	$279 = 2^{34} \bmod(2027)$	$329 = 2^{536} \bmod(2027)$
$230 = 2^{1951} \bmod(2027)$	$280 = 2^{1701} \bmod(2027)$	$330 = 2^{1537} \bmod(2027)$
$231 = 2^{1322} \bmod(2027)$	$281 = 2^{1511} \bmod(2027)$	$331 = 2^{824} \bmod(2027)$
$232 = 2^{612} \bmod(2027)$	$282 = 2^{1090} \bmod(2027)$	$332 = 2^{402} \bmod(2027)$
$233 = 2^{1135} \bmod(2027)$	$283 = 2^{1266} \bmod(2027)$	$333 = 2^{1339} \bmod(2027)$
$234 = 2^{423} \bmod(2027)$	$284 = 2^{1424} \bmod(2027)$	$334 = 2^{711} \bmod(2027)$
$235 = 2^{750} \bmod(2027)$	$285 = 2^{1289} \bmod(2027)$	$335 = 2^{360} \bmod(2027)$
$236 = 2^{1395} \bmod(2027)$	$286 = 2^{1170} \bmod(2027)$	$336 = 2^{15} \bmod(2027)$
$237 = 2^{1269} \bmod(2027)$	$287 = 2^{1849} \bmod(2027)$	$337 = 2^{673} \bmod(2027)$
$238 = 2^{1386} \bmod(2027)$	$288 = 2^{569} \bmod(2027)$	$338 = 2^{1743} \bmod(2027)$
$239 = 2^{934} \bmod(2027)$	$289 = 2^{1286} \bmod(2027)$	$339 = 2^{1472} \bmod(2027)$
$240 = 2^{229} \bmod(2027)$	$290 = 2^{553} \bmod(2027)$	$340 = 2^{1601} \bmod(2027)$
$241 = 2^{859} \bmod(2027)$	$291 = 2^{215} \bmod(2027)$	$341 = 2^{781} \bmod(2027)$
$242 = 2^{597} \bmod(2027)$	$292 = 2^{1927} \bmod(2027)$	$342 = 2^{1629} \bmod(2027)$
$243 = 2^{1410} \bmod(2027)$	$293 = 2^{556} \bmod(2027)$	$343 = 2^{1213} \bmod(2027)$
$244 = 2^{1178} \bmod(2027)$	$294 = 2^{1767} \bmod(2027)$	$344 = 2^{492} \bmod(2027)$
$245 = 2^{1427} \bmod(2027)$	$295 = 2^{1336} \bmod(2027)$	$345 = 2^{206} \bmod(2027)$
$246 = 2^{377} \bmod(2027)$	$296 = 2^{778} \bmod(2027)$	$346 = 2^{1201} \bmod(2027)$
$247 = 2^{922} \bmod(2027)$	$297 = 2^{131} \bmod(2027)$	$347 = 2^{971} \bmod(2027)$
$248 = 2^{1499} \bmod(2027)$	$298 = 2^{1664} \bmod(2027)$	$348 = 2^{893} \bmod(2027)$
$249 = 2^{682} \bmod(2027)$	$299 = 2^{1865} \bmod(2027)$	$349 = 2^{134} \bmod(2027)$
$250 = 2^{1856} \bmod(2027)$	$300 = 2^{170} \bmod(2027)$	$350 = 2^{1642} \bmod(2027)$
$251 = 2^{48} \bmod(2027)$	$301 = 2^{218} \bmod(2027)$	$351 = 2^{704} \bmod(2027)$
$252 = 2^{295} \bmod(2027)$	$302 = 2^{1162} \bmod(2027)$	$352 = 2^{1316} \bmod(2027)$
$253 = 2^{1292} \bmod(2027)$	$303 = 2^{1079} \bmod(2027)$	$353 = 2^{1330} \bmod(2027)$
$254 = 2^{1966} \bmod(2027)$	$304 = 2^{1068} \bmod(2027)$	$354 = 2^{1676} \bmod(2027)$
$255 = 2^{1881} \bmod(2027)$	$305 = 2^{1119} \bmod(2027)$	$355 = 2^{1365} \bmod(2027)$
$256 = 2^8 \bmod(2027)$	$306 = 2^{195} \bmod(2027)$	$356 = 2^{1992} \bmod(2027)$
$257 = 2^{606} \bmod(2027)$	$307 = 2^{1448} \bmod(2027)$	$357 = 2^{1667} \bmod(2027)$
$258 = 2^{772} \bmod(2027)$	$308 = 2^{1042} \bmod(2027)$	$358 = 2^{313} \bmod(2027)$
$259 = 2^{504} \bmod(2027)$	$309 = 2^{1930} \bmod(2027)$	$359 = 2^{1682} \bmod(2027)$
$260 = 2^{1829} \bmod(2027)$	$310 = 2^{1440} \bmod(2027)$	$360 = 2^{510} \bmod(2027)$
$261 = 2^{1173} \bmod(2027)$	$311 = 2^{440} \bmod(2027)$	$361 = 2^{102} \bmod(2027)$
$262 = 2^{260} \bmod(2027)$	$312 = 2^{143} \bmod(2027)$	$362 = 2^{269} \bmod(2027)$
$263 = 2^{1037} \bmod(2027)$	$313 = 2^{367} \bmod(2027)$	$363 = 2^{878} \bmod(2027)$

$364 = 2^{1615} \text{mod}(2027)$	$414 = 2^{546} \text{mod}(2027)$	$464 = 2^{613} \text{mod}(2027)$
$365 = 2^{1868} \text{mod}(2027)$	$415 = 2^{343} \text{mod}(2027)$	$465 = 2^{1721} \text{mod}(2027)$
$366 = 2^{1459} \text{mod}(2027)$	$416 = 2^{1889} \text{mod}(2027)$	$466 = 2^{1136} \text{mod}(2027)$
$367 = 2^{1358} \text{mod}(2027)$	$417 = 2^{667} \text{mod}(2027)$	$467 = 2^{1099} \text{mod}(2027)$
$368 = 2^{2011} \text{mod}(2027)$	$418 = 2^{350} \text{mod}(2027)$	$468 = 2^{424} \text{mod}(2027)$
$369 = 2^{658} \text{mod}(2027)$	$419 = 2^{1715} \text{mod}(2027)$	$469 = 2^{146} \text{mod}(2027)$
$370 = 2^{719} \text{mod}(2027)$	$420 = 2^{1982} \text{mod}(2027)$	$470 = 2^{751} \text{mod}(2027)$
$371 = 2^{1561} \text{mod}(2027)$	$421 = 2^{198} \text{mod}(2027)$	$471 = 2^{154} \text{mod}(2027)$
$372 = 2^{1780} \text{mod}(2027)$	$422 = 2^{457} \text{mod}(2027)$	$472 = 2^{1396} \text{mod}(2027)$
$373 = 2^{173} \text{mod}(2027)$	$423 = 2^{1371} \text{mod}(2027)$	$473 = 2^{1800} \text{mod}(2027)$
$374 = 2^{942} \text{mod}(2027)$	$424 = 2^{1835} \text{mod}(2027)$	$474 = 2^{1270} \text{mod}(2027)$
$375 = 2^{111} \text{mod}(2027)$	$425 = 2^{1542} \text{mod}(2027)$	$475 = 2^{950} \text{mod}(2027)$
$376 = 2^{810} \text{mod}(2027)$	$426 = 2^{1705} \text{mod}(2027)$	$476 = 2^{1387} \text{mod}(2027)$
$377 = 2^{467} \text{mod}(2027)$	$427 = 2^{905} \text{mod}(2027)$	$477 = 2^{370} \text{mod}(2027)$
$378 = 2^{576} \text{mod}(2027)$	$428 = 2^{1247} \text{mod}(2027)$	$478 = 2^{935} \text{mod}(2027)$
$379 = 2^{639} \text{mod}(2027)$	$429 = 2^{1451} \text{mod}(2027)$	$479 = 2^{42} \text{mod}(2027)$
$380 = 2^{1009} \text{mod}(2027)$	$430 = 2^{433} \text{mod}(2027)$	$480 = 2^{230} \text{mod}(2027)$
$381 = 2^{221} \text{mod}(2027)$	$431 = 2^{64} \text{mod}(2027)$	$481 = 2^{633} \text{mod}(2027)$
$382 = 2^{1492} \text{mod}(2027)$	$432 = 2^{850} \text{mod}(2027)$	$482 = 2^{860} \text{mod}(2027)$
$383 = 2^{803} \text{mod}(2027)$	$433 = 2^{321} \text{mod}(2027)$	$483 = 2^{2018} \text{mod}(2027)$
$384 = 2^{289} \text{mod}(2027)$	$434 = 2^{1226} \text{mod}(2027)$	$484 = 2^{598} \text{mod}(2027)$
$385 = 2^{983} \text{mod}(2027)$	$435 = 2^{834} \text{mod}(2027)$	$485 = 2^{1902} \text{mod}(2027)$
$386 = 2^{1003} \text{mod}(2027)$	$436 = 2^{251} \text{mod}(2027)$	$486 = 2^{1411} \text{mod}(2027)$
$387 = 2^{1053} \text{mod}(2027)$	$437 = 2^{1045} \text{mod}(2027)$	$487 = 2^{1998} \text{mod}(2027)$
$388 = 2^{1961} \text{mod}(2027)$	$438 = 2^{182} \text{mod}(2027)$	$488 = 2^{1179} \text{mod}(2027)$
$389 = 2^{1165} \text{mod}(2027)$	$439 = 2^{71} \text{mod}(2027)$	$489 = 2^{407} \text{mod}(2027)$
$390 = 2^{84} \text{mod}(2027)$	$440 = 2^{1257} \text{mod}(2027)$	$490 = 2^{1428} \text{mod}(2027)$
$391 = 2^{1637} \text{mod}(2027)$	$441 = 2^{22} \text{mod}(2027)$	$491 = 2^{1304} \text{mod}(2027)$
$392 = 2^{1487} \text{mod}(2027)$	$442 = 2^{1515} \text{mod}(2027)$	$492 = 2^{378} \text{mod}(2027)$
$393 = 2^{541} \text{mod}(2027)$	$443 = 2^{866} \text{mod}(2027)$	$493 = 2^{239} \text{mod}(2027)$
$394 = 2^{390} \text{mod}(2027)$	$444 = 2^{1059} \text{mod}(2027)$	$494 = 2^{923} \text{mod}(2027)$
$395 = 2^{930} \text{mod}(2027)$	$445 = 2^{1933} \text{mod}(2027)$	$495 = 2^{1818} \text{mod}(2027)$
$396 = 2^{1877} \text{mod}(2027)$	$446 = 2^{395} \text{mod}(2027)$	$496 = 2^{1500} \text{mod}(2027)$
$397 = 2^{1082} \text{mod}(2027)$	$447 = 2^{1945} \text{mod}(2027)$	$497 = 2^{1151} \text{mod}(2027)$
$398 = 2^{1845} \text{mod}(2027)$	$448 = 2^{1761} \text{mod}(2027)$	$498 = 2^{683} \text{mod}(2027)$
$399 = 2^{1075} \text{mod}(2027)$	$449 = 2^{307} \text{mod}(2027)$	$499 = 2^{481} \text{mod}(2027)$
$400 = 2^{1916} \text{mod}(2027)$	$450 = 2^{451} \text{mod}(2027)$	$500 = 2^{1857} \text{mod}(2027)$
$401 = 2^{356} \text{mod}(2027)$	$451 = 2^{1405} \text{mod}(2027)$	$501 = 2^{992} \text{mod}(2027)$
$402 = 2^{700} \text{mod}(2027)$	$452 = 2^{1192} \text{mod}(2027)$	$502 = 2^{49} \text{mod}(2027)$
$403 = 2^{1354} \text{mod}(2027)$	$453 = 2^{1443} \text{mod}(2027)$	$503 = 2^{1236} \text{mod}(2027)$
$404 = 2^{799} \text{mod}(2027)$	$454 = 2^{1467} \text{mod}(2027)$	$504 = 2^{296} \text{mod}(2027)$
$405 = 2^{1071} \text{mod}(2027)$	$455 = 2^{1556} \text{mod}(2027)$	$505 = 2^{740} \text{mod}(2027)$
$406 = 2^{339} \text{mod}(2027)$	$456 = 2^{1349} \text{mod}(2027)$	$506 = 2^{1293} \text{mod}(2027)$
$407 = 2^{60} \text{mod}(2027)$	$457 = 2^{829} \text{mod}(2027)$	$507 = 2^{2024} \text{mod}(2027)$
$408 = 2^{1941} \text{mod}(2027)$	$458 = 2^{1094} \text{mod}(2027)$	$508 = 2^{1967} \text{mod}(2027)$
$409 = 2^{622} \text{mod}(2027)$	$459 = 2^{476} \text{mod}(2027)$	$509 = 2^{562} \text{mod}(2027)$
$410 = 2^{38} \text{mod}(2027)$	$460 = 2^{1952} \text{mod}(2027)$	$510 = 2^{1882} \text{mod}(2027)$
$411 = 2^{1814} \text{mod}(2027)$	$461 = 2^{443} \text{mod}(2027)$	$511 = 2^{1654} \text{mod}(2027)$
$412 = 2^{1650} \text{mod}(2027)$	$462 = 2^{1323} \text{mod}(2027)$	$512 = 2^9 \text{mod}(2027)$
$413 = 2^{1122} \text{mod}(2027)$	$463 = 2^{626} \text{mod}(2027)$	$513 = 2^{1910} \text{mod}(2027)$

$514 = 2^{607} \bmod(2027)$	$564 = 2^{1091} \bmod(2027)$	$614 = 2^{1449} \bmod(2027)$
$515 = 2^{1591} \bmod(2027)$	$565 = 2^{1133} \bmod(2027)$	$615 = 2^{319} \bmod(2027)$
$516 = 2^{773} \bmod(2027)$	$566 = 2^{1267} \bmod(2027)$	$616 = 2^{1043} \bmod(2027)$
$517 = 2^{92} \bmod(2027)$	$567 = 2^{857} \bmod(2027)$	$617 = 2^{20} \bmod(2027)$
$518 = 2^{505} \bmod(2027)$	$568 = 2^{1425} \bmod(2027)$	$618 = 2^{1931} \bmod(2027)$
$519 = 2^{1482} \bmod(2027)$	$569 = 2^{680} \bmod(2027)$	$619 = 2^{305} \bmod(2027)$
$520 = 2^{1830} \bmod(2027)$	$570 = 2^{1290} \bmod(2027)$	$620 = 2^{1441} \bmod(2027)$
$521 = 2^{1344} \bmod(2027)$	$571 = 2^{604} \bmod(2027)$	$621 = 2^{827} \bmod(2027)$
$522 = 2^{1174} \bmod(2027)$	$572 = 2^{1171} \bmod(2027)$	$622 = 2^{441} \bmod(2027)$
$523 = 2^{1825} \bmod(2027)$	$573 = 2^{1773} \bmod(2027)$	$623 = 2^{1719} \bmod(2027)$
$524 = 2^{261} \bmod(2027)$	$574 = 2^{1850} \bmod(2027)$	$624 = 2^{144} \bmod(2027)$
$525 = 2^{1923} \bmod(2027)$	$575 = 2^{1893} \bmod(2027)$	$625 = 2^{1798} \bmod(2027)$
$526 = 2^{1038} \bmod(2027)$	$576 = 2^{570} \bmod(2027)$	$626 = 2^{368} \bmod(2027)$
$527 = 2^{1126} \bmod(2027)$	$577 = 2^{1509} \bmod(2027)$	$627 = 2^{631} \bmod(2027)$
$528 = 2^{1597} \bmod(2027)$	$578 = 2^{1287} \bmod(2027)$	$628 = 2^{1900} \bmod(2027)$
$529 = 2^{1988} \bmod(2027)$	$579 = 2^{1284} \bmod(2027)$	$629 = 2^{405} \bmod(2027)$
$530 = 2^{1776} \bmod(2027)$	$580 = 2^{554} \bmod(2027)$	$630 = 2^{237} \bmod(2027)$
$531 = 2^{1957} \bmod(2027)$	$581 = 2^{129} \bmod(2027)$	$631 = 2^{1149} \bmod(2027)$
$532 = 2^{795} \bmod(2027)$	$582 = 2^{216} \bmod(2027)$	$632 = 2^{990} \bmod(2027)$
$533 = 2^{1978} \bmod(2027)$	$583 = 2^{1117} \bmod(2027)$	$633 = 2^{738} \bmod(2027)$
$534 = 2^{247} \bmod(2027)$	$584 = 2^{1928} \bmod(2027)$	$634 = 2^{560} \bmod(2027)$
$535 = 2^{1188} \bmod(2027)$	$585 = 2^{365} \bmod(2027)$	$635 = 2^{1908} \bmod(2027)$
$536 = 2^{420} \bmod(2027)$	$586 = 2^{557} \bmod(2027)$	$636 = 2^{90} \bmod(2027)$
$537 = 2^{594} \bmod(2027)$	$587 = 2^{1525} \bmod(2027)$	$637 = 2^{1342} \bmod(2027)$
$538 = 2^{1853} \bmod(2027)$	$588 = 2^{1768} \bmod(2027)$	$638 = 2^{1921} \bmod(2027)$
$539 = 2^{769} \bmod(2027)$	$589 = 2^{534} \bmod(2027)$	$639 = 2^{1986} \bmod(2027)$
$540 = 2^{791} \bmod(2027)$	$590 = 2^{1337} \bmod(2027)$	$640 = 2^{1976} \bmod(2027)$
$541 = 2^{1530} \bmod(2027)$	$591 = 2^{671} \bmod(2027)$	$641 = 2^{592} \bmod(2027)$
$542 = 2^{1087} \bmod(2027)$	$592 = 2^{779} \bmod(2027)$	$642 = 2^{1528} \bmod(2027)$
$543 = 2^{550} \bmod(2027)$	$593 = 2^{204} \bmod(2027)$	$643 = 2^{190} \bmod(2027)$
$544 = 2^{1661} \bmod(2027)$	$594 = 2^{132} \bmod(2027)$	$644 = 2^{1738} \bmod(2027)$
$545 = 2^{192} \bmod(2027)$	$595 = 2^{1328} \bmod(2027)$	$645 = 2^{714} \bmod(2027)$
$546 = 2^{1896} \bmod(2027)$	$596 = 2^{1665} \bmod(2027)$	$646 = 2^{695} \bmod(2027)$
$547 = 2^{1734} \bmod(2027)$	$597 = 2^{100} \bmod(2027)$	$647 = 2^{1221} \bmod(2027)$
$548 = 2^{1534} \bmod(2027)$	$598 = 2^{1866} \bmod(2027)$	$648 = 2^{1131} \bmod(2027)$
$549 = 2^{1740} \bmod(2027)$	$599 = 2^{656} \bmod(2027)$	$649 = 2^{678} \bmod(2027)$
$550 = 2^{1198} \bmod(2027)$	$600 = 2^{171} \bmod(2027)$	$650 = 2^{1771} \bmod(2027)$
$551 = 2^{1673} \bmod(2027)$	$601 = 2^{465} \bmod(2027)$	$651 = 2^{1507} \bmod(2027)$
$552 = 2^{266} \bmod(2027)$	$602 = 2^{219} \bmod(2027)$	$652 = 2^{127} \bmod(2027)$
$553 = 2^{716} \bmod(2027)$	$603 = 2^{981} \bmod(2027)$	$653 = 2^{363} \bmod(2027)$
$554 = 2^{573} \bmod(2027)$	$604 = 2^{1163} \bmod(2027)$	$654 = 2^{532} \bmod(2027)$
$555 = 2^{1000} \bmod(2027)$	$605 = 2^{539} \bmod(2027)$	$655 = 2^{202} \bmod(2027)$
$556 = 2^{387} \bmod(2027)$	$606 = 2^{1080} \bmod(2027)$	$656 = 2^{98} \bmod(2027)$
$557 = 2^{697} \bmod(2027)$	$607 = 2^{354} \bmod(2027)$	$657 = 2^{463} \bmod(2027)$
$558 = 2^{35} \bmod(2027)$	$608 = 2^{1069} \bmod(2027)$	$658 = 2^{537} \bmod(2027)$
$559 = 2^{347} \bmod(2027)$	$609 = 2^{620} \bmod(2027)$	$659 = 2^{618} \bmod(2027)$
$560 = 2^{1702} \bmod(2027)$	$610 = 2^{1120} \bmod(2027)$	$660 = 2^{1538} \bmod(2027)$
$561 = 2^{1223} \bmod(2027)$	$611 = 2^{665} \bmod(2027)$	$661 = 2^{18} \bmod(2027)$
$562 = 2^{1512} \bmod(2027)$	$612 = 2^{196} \bmod(2027)$	$662 = 2^{825} \bmod(2027)$
$563 = 2^{448} \bmod(2027)$	$613 = 2^{1540} \bmod(2027)$	$663 = 2^{1796} \bmod(2027)$

$664 = 2^{403} \bmod(2027)$	$714 = 2^{1668} \bmod(2027)$	$764 = 2^{1493} \bmod(2027)$
$665 = 2^{736} \bmod(2027)$	$715 = 2^{1112} \bmod(2027)$	$765 = 2^{137} \bmod(2027)$
$666 = 2^{1340} \bmod(2027)$	$716 = 2^{314} \bmod(2027)$	$766 = 2^{804} \bmod(2027)$
$667 = 2^{590} \bmod(2027)$	$717 = 2^{1216} \bmod(2027)$	$767 = 2^{1251} \bmod(2027)$
$668 = 2^{712} \bmod(2027)$	$718 = 2^{1683} \bmod(2027)$	$768 = 2^{290} \bmod(2027)$
$669 = 2^{676} \bmod(2027)$	$719 = 2^{1546} \bmod(2027)$	$769 = 2^{1419} \bmod(2027)$
$670 = 2^{361} \bmod(2027)$	$720 = 2^{511} \bmod(2027)$	$770 = 2^{984} \bmod(2027)$
$671 = 2^{461} \bmod(2027)$	$721 = 2^{1377} \bmod(2027)$	$771 = 2^{888} \bmod(2027)$
$672 = 2^{16} \bmod(2027)$	$722 = 2^{103} \bmod(2027)$	$772 = 2^{1004} \bmod(2027)$
$673 = 2^{734} \bmod(2027)$	$723 = 2^{1141} \bmod(2027)$	$773 = 2^{1645} \bmod(2027)$
$674 = 2^{674} \bmod(2027)$	$724 = 2^{270} \bmod(2027)$	$774 = 2^{1054} \bmod(2027)$
$675 = 2^{732} \bmod(2027)$	$725 = 2^{495} \bmod(2027)$	$775 = 2^{1382} \bmod(2027)$
$676 = 2^{1744} \bmod(2027)$	$726 = 2^{879} \bmod(2027)$	$776 = 2^{1962} \bmod(2027)$
$677 = 2^{1746} \bmod(2027)$	$727 = 2^{759} \bmod(2027)$	$777 = 2^{786} \bmod(2027)$
$678 = 2^{1473} \bmod(2027)$	$728 = 2^{1616} \bmod(2027)$	$778 = 2^{1166} \bmod(2027)$
$679 = 2^{1688} \bmod(2027)$	$729 = 2^{1692} \bmod(2027)$	$779 = 2^{1158} \bmod(2027)$
$680 = 2^{1602} \bmod(2027)$	$730 = 2^{1869} \bmod(2027)$	$780 = 2^{85} \bmod(2027)$
$681 = 2^{1748} \bmod(2027)$	$731 = 2^{119} \bmod(2027)$	$781 = 2^{707} \bmod(2027)$
$682 = 2^{782} \bmod(2027)$	$732 = 2^{1460} \bmod(2027)$	$782 = 2^{1638} \bmod(2027)$
$683 = 2^{1030} \bmod(2027)$	$733 = 2^{209} \bmod(2027)$	$783 = 2^{1455} \bmod(2027)$
$684 = 2^{1630} \bmod(2027)$	$734 = 2^{1359} \bmod(2027)$	$784 = 2^{1488} \bmod(2027)$
$685 = 2^{1475} \bmod(2027)$	$735 = 2^{1709} \bmod(2027)$	$785 = 2^{1841} \bmod(2027)$
$686 = 2^{1214} \bmod(2027)$	$736 = 2^{2012} \bmod(2027)$	$786 = 2^{542} \bmod(2027)$
$687 = 2^{1375} \bmod(2027)$	$737 = 2^{1728} \bmod(2027)$	$787 = 2^{429} \bmod(2027)$
$688 = 2^{493} \bmod(2027)$	$738 = 2^{659} \bmod(2027)$	$788 = 2^{391} \bmod(2027)$
$689 = 2^{1690} \bmod(2027)$	$739 = 2^{726} \bmod(2027)$	$789 = 2^{1319} \bmod(2027)$
$690 = 2^{207} \bmod(2027)$	$740 = 2^{720} \bmod(2027)$	$790 = 2^{931} \bmod(2027)$
$691 = 2^{1726} \bmod(2027)$	$741 = 2^{1204} \bmod(2027)$	$791 = 2^{919} \bmod(2027)$
$692 = 2^{1202} \bmod(2027)$	$742 = 2^{1562} \bmod(2027)$	$792 = 2^{1878} \bmod(2027)$
$693 = 2^{1604} \bmod(2027)$	$743 = 2^{516} \bmod(2027)$	$793 = 2^{1034} \bmod(2027)$
$694 = 2^{972} \bmod(2027)$	$744 = 2^{1781} \bmod(2027)$	$794 = 2^{1083} \bmod(2027)$
$695 = 2^{328} \bmod(2027)$	$745 = 2^{1606} \bmod(2027)$	$795 = 2^{31} \bmod(2027)$
$696 = 2^{894} \bmod(2027)$	$746 = 2^{174} \bmod(2027)$	$796 = 2^{1846} \bmod(2027)$
$697 = 2^{1750} \bmod(2027)$	$747 = 2^{964} \bmod(2027)$	$797 = 2^{1333} \bmod(2027)$
$698 = 2^{135} \bmod(2027)$	$748 = 2^{943} \bmod(2027)$	$798 = 2^{1076} \bmod(2027)$
$699 = 2^{1417} \bmod(2027)$	$749 = 2^{974} \bmod(2027)$	$799 = 2^{437} \bmod(2027)$
$700 = 2^{1643} \bmod(2027)$	$750 = 2^{112} \bmod(2027)$	$800 = 2^{1917} \bmod(2027)$
$701 = 2^{784} \bmod(2027)$	$751 = 2^{909} \bmod(2027)$	$801 = 2^{528} \bmod(2027)$
$702 = 2^{705} \bmod(2027)$	$752 = 2^{811} \bmod(2027)$	$802 = 2^{357} \bmod(2027)$
$703 = 2^{1839} \bmod(2027)$	$753 = 2^{330} \bmod(2027)$	$803 = 2^{1210} \bmod(2027)$
$704 = 2^{1317} \bmod(2027)$	$754 = 2^{468} \bmod(2027)$	$804 = 2^{701} \bmod(2027)$
$705 = 2^{1032} \bmod(2027)$	$755 = 2^{1104} \bmod(2027)$	$805 = 2^{1679} \bmod(2027)$
$706 = 2^{1331} \bmod(2027)$	$756 = 2^{577} \bmod(2027)$	$806 = 2^{1355} \bmod(2027)$
$707 = 2^{526} \bmod(2027)$	$757 = 2^{896} \bmod(2027)$	$807 = 2^{108} \bmod(2027)$
$708 = 2^{1677} \bmod(2027)$	$758 = 2^{640} \bmod(2027)$	$808 = 2^{800} \bmod(2027)$
$709 = 2^{1632} \bmod(2027)$	$759 = 2^{1574} \bmod(2027)$	$809 = 2^{1634} \bmod(2027)$
$710 = 2^{1366} \bmod(2027)$	$760 = 2^{1010} \bmod(2027)$	$810 = 2^{1072} \bmod(2027)$
$711 = 2^{1551} \bmod(2027)$	$761 = 2^{1752} \bmod(2027)$	$811 = 2^{57} \bmod(2027)$
$712 = 2^{1993} \bmod(2027)$	$762 = 2^{222} \bmod(2027)$	$812 = 2^{340} \bmod(2027)$
$713 = 2^{1477} \bmod(2027)$	$763 = 2^{2004} \bmod(2027)$	$813 = 2^{1368} \bmod(2027)$



$814 = 2^{61} \bmod(2077)$	$864 = 2^{851} \bmod(2077)$	$914 = 2^{830} \bmod(2077)$
$815 = 2^{68} \bmod(2077)$	$865 = 2^{1143} \bmod(2077)$	$915 = 2^{1401} \bmod(2077)$
$816 = 2^{1942} \bmod(2077)$	$866 = 2^{322} \bmod(2077)$	$916 = 2^{1095} \bmod(2077)$
$817 = 2^{1553} \bmod(2077)$	$867 = 2^{1568} \bmod(2077)$	$917 = 2^{2014} \bmod(2077)$
$818 = 2^{623} \bmod(2077)$	$868 = 2^{1227} \bmod(2077)$	$918 = 2^{477} \bmod(2077)$
$819 = 2^{151} \bmod(2077)$	$869 = 2^{272} \bmod(2077)$	$919 = 2^{1587} \bmod(2077)$
$820 = 2^{39} \bmod(2077)$	$870 = 2^{835} \bmod(2077)$	$920 = 2^{1953} \bmod(2077)$
$821 = 2^{1995} \bmod(2077)$	$871 = 2^{275} \bmod(2077)$	$921 = 2^{1730} \bmod(2077)$
$822 = 2^{1815} \bmod(2077)$	$872 = 2^{252} \bmod(2077)$	$922 = 2^{444} \bmod(2077)$
$823 = 2^{1233} \bmod(2077)$	$873 = 2^{497} \bmod(2077)$	$923 = 2^{1280} \bmod(2077)$
$824 = 2^{1651} \bmod(2077)$	$874 = 2^{1046} \bmod(2077)$	$924 = 2^{1324} \bmod(2077)$
$825 = 2^{1479} \bmod(2077)$	$875 = 2^{1584} \bmod(2077)$	$925 = 2^{661} \bmod(2077)$
$826 = 2^{1123} \bmod(2077)$	$876 = 2^{183} \bmod(2077)$	$926 = 2^{627} \bmod(2077)$
$827 = 2^{1185} \bmod(2077)$	$877 = 2^{881} \bmod(2077)$	$927 = 2^{186} \bmod(2077)$
$828 = 2^{547} \bmod(2077)$	$878 = 2^{72} \bmod(2077)$	$928 = 2^{614} \bmod(2077)$
$829 = 2^{1670} \bmod(2077)$	$879 = 2^{838} \bmod(2077)$	$929 = 2^{728} \bmod(2077)$
$830 = 2^{344} \bmod(2077)$	$880 = 2^{1258} \bmod(2077)$	$930 = 2^{1722} \bmod(2077)$
$831 = 2^{854} \bmod(2077)$	$881 = 2^{761} \bmod(2077)$	$931 = 2^{522} \bmod(2077)$
$832 = 2^{1890} \bmod(2077)$	$882 = 2^{23} \bmod(2077)$	$932 = 2^{1137} \bmod(2077)$
$833 = 2^{1114} \bmod(2077)$	$883 = 2^{159} \bmod(2077)$	$933 = 2^{722} \bmod(2077)$
$834 = 2^{668} \bmod(2077)$	$884 = 2^{1516} \bmod(2077)$	$934 = 2^{1100} \bmod(2077)$
$835 = 2^{653} \bmod(2077)$	$885 = 2^{1618} \bmod(2077)$	$935 = 2^{884} \bmod(2077)$
$836 = 2^{351} \bmod(2077)$	$886 = 2^{867} \bmod(2077)$	$936 = 2^{425} \bmod(2077)$
$837 = 2^{316} \bmod(2077)$	$887 = 2^{278} \bmod(2077)$	$937 = 2^{1206} \bmod(2077)$
$838 = 2^{1716} \bmod(2077)$	$888 = 2^{1060} \bmod(2077)$	$938 = 2^{147} \bmod(2077)$
$839 = 2^{1146} \bmod(2077)$	$889 = 2^{1694} \bmod(2077)$	$939 = 2^{649} \bmod(2077)$
$840 = 2^{1983} \bmod(2077)$	$890 = 2^{1934} \bmod(2077)$	$940 = 2^{752} \bmod(2077)$
$841 = 2^{1218} \bmod(2077)$	$891 = 2^{413} \bmod(2077)$	$941 = 2^{1564} \bmod(2077)$
$842 = 2^{199} \bmod(2077)$	$892 = 2^{396} \bmod(2077)$	$942 = 2^{155} \bmod(2077)$
$843 = 2^{1793} \bmod(2077)$	$893 = 2^{1871} \bmod(2077)$	$943 = 2^{75} \bmod(2077)$
$844 = 2^{458} \bmod(2077)$	$894 = 2^{1946} \bmod(2077)$	$944 = 2^{1397} \bmod(2077)$
$845 = 2^{1685} \bmod(2077)$	$895 = 2^{255} \bmod(2077)$	$945 = 2^{518} \bmod(2077)$
$846 = 2^{1372} \bmod(2077)$	$896 = 2^{1762} \bmod(2077)$	$946 = 2^{1801} \bmod(2077)$
$847 = 2^{325} \bmod(2077)$	$897 = 2^{121} \bmod(2077)$	$947 = 2^{1805} \bmod(2077)$
$848 = 2^{1836} \bmod(2077)$	$898 = 2^{308} \bmod(2077)$	$948 = 2^{1271} \bmod(2077)$
$849 = 2^{1548} \bmod(2077)$	$899 = 2^{79} \bmod(2077)$	$949 = 2^{1783} \bmod(2077)$
$850 = 2^{1543} \bmod(2077)$	$900 = 2^{452} \bmod(2077)$	$950 = 2^{951} \bmod(2077)$
$851 = 2^{756} \bmod(2077)$	$901 = 2^{1462} \bmod(2077)$	$951 = 2^{841} \bmod(2077)$
$852 = 2^{1706} \bmod(2077)$	$902 = 2^{1406} \bmod(2077)$	$952 = 2^{1388} \bmod(2077)$
$853 = 2^{513} \bmod(2077)$	$903 = 2^{500} \bmod(2077)$	$953 = 2^{1608} \bmod(2077)$
$854 = 2^{906} \bmod(2077)$	$904 = 2^{1193} \bmod(2077)$	$954 = 2^{371} \bmod(2077)$
$855 = 2^{1571} \bmod(2077)$	$905 = 2^{211} \bmod(2077)$	$955 = 2^{1434} \bmod(2077)$
$856 = 2^{1248} \bmod(2077)$	$906 = 2^{1444} \bmod(2077)$	$956 = 2^{936} \bmod(2077)$
$857 = 2^{1379} \bmod(2077)$	$907 = 2^{690} \bmod(2077)$	$957 = 2^{176} \bmod(2077)$
$858 = 2^{1452} \bmod(2077)$	$908 = 2^{1468} \bmod(2077)$	$958 = 2^{43} \bmod(2077)$
$859 = 2^{916} \bmod(2077)$	$909 = 2^{1361} \bmod(2077)$	$959 = 2^{1261} \bmod(2077)$
$860 = 2^{434} \bmod(2077)$	$910 = 2^{1557} \bmod(2077)$	$960 = 2^{231} \bmod(2077)$
$861 = 2^{105} \bmod(2077)$	$911 = 2^{1049} \bmod(2077)$	$961 = 2^{966} \bmod(2077)$
$862 = 2^{65} \bmod(2077)$	$912 = 2^{1350} \bmod(2077)$	$962 = 2^{634} \bmod(2077)$
$863 = 2^{1230} \bmod(2077)$	$913 = 2^{1711} \bmod(2077)$	$963 = 2^{1809} \bmod(2077)$

$964 = 2^{861} \bmod(2027)$	$1014 = 2^{2025} \bmod(2027)$	$1064 = 2^{796} \bmod(2027)$
$965 = 2^{945} \bmod(2027)$	$1015 = 2^{281} \bmod(2027)$	$1065 = 2^{1647} \bmod(2027)$
$966 = 2^{2019} \bmod(2027)$	$1016 = 2^{1968} \bmod(2027)$	$1066 = 2^{1979} \bmod(2027)$
$967 = 2^{764} \bmod(2027)$	$1017 = 2^{1754} \bmod(2027)$	$1067 = 2^{1244} \bmod(2027)$
$968 = 2^{599} \bmod(2027)$	$1018 = 2^{563} \bmod(2027)$	$1068 = 2^{248} \bmod(2027)$
$969 = 2^{976} \bmod(2027)$	$1019 = 2^{1310} \bmod(2027)$	$1069 = 2^{1056} \bmod(2027)$
$970 = 2^{1903} \bmod(2027)$	$1020 = 2^{1883} \bmod(2027)$	$1070 = 2^{1189} \bmod(2027)$
$971 = 2^{585} \bmod(2027)$	$1021 = 2^{224} \bmod(2027)$	$1071 = 2^{1949} \bmod(2027)$
$972 = 2^{1412} \bmod(2027)$	$1022 = 2^{1655} \bmod(2027)$	$1072 = 2^{421} \bmod(2027)$
$973 = 2^{114} \bmod(2027)$	$1023 = 2^{1063} \bmod(2027)$	$1073 = 2^{1384} \bmod(2027)$
$974 = 2^{1999} \bmod(2027)$	$1024 = 2^{10} \bmod(2027)$	$1074 = 2^{595} \bmod(2027)$
$975 = 2^{26} \bmod(2027)$	$1025 = 2^{2006} \bmod(2027)$	$1075 = 2^{375} \bmod(2027)$
$976 = 2^{1180} \bmod(2027)$	$1026 = 2^{1911} \bmod(2027)$	$1076 = 2^{1854} \bmod(2027)$
$977 = 2^{911} \bmod(2027)$	$1027 = 2^{845} \bmod(2027)$	$1077 = 2^{1964} \bmod(2027)$
$978 = 2^{408} \bmod(2027)$	$1028 = 2^{608} \bmod(2027)$	$1078 = 2^{770} \bmod(2027)$
$979 = 2^{1275} \bmod(2027)$	$1029 = 2^{1495} \bmod(2027)$	$1079 = 2^{258} \bmod(2027)$
$980 = 2^{1429} \bmod(2027)$	$1030 = 2^{1592} \bmod(2027)$	$1080 = 2^{792} \bmod(2027)$
$981 = 2^{813} \bmod(2027)$	$1031 = 2^{1697} \bmod(2027)$	$1081 = 2^{788} \bmod(2027)$
$982 = 2^{1305} \bmod(2027)$	$1032 = 2^{774} \bmod(2027)$	$1082 = 2^{1531} \bmod(2027)$
$983 = 2^{162} \bmod(2027)$	$1033 = 2^{139} \bmod(2027)$	$1083 = 2^{384} \bmod(2027)$
$984 = 2^{379} \bmod(2027)$	$1034 = 2^{93} \bmod(2027)$	$1084 = 2^{1088} \bmod(2027)$
$985 = 2^{332} \bmod(2027)$	$1035 = 2^{488} \bmod(2027)$	$1085 = 2^{1168} \bmod(2027)$
$986 = 2^{240} \bmod(2027)$	$1036 = 2^{506} \bmod(2027)$	$1086 = 2^{551} \bmod(2027)$
$987 = 2^{818} \bmod(2027)$	$1037 = 2^{806} \bmod(2027)$	$1087 = 2^{1765} \bmod(2027)$
$988 = 2^{924} \bmod(2027)$	$1038 = 2^{1483} \bmod(2027)$	$1088 = 2^{1662} \bmod(2027)$
$989 = 2^{470} \bmod(2027)$	$1039 = 2^{1937} \bmod(2027)$	$1089 = 2^{1160} \bmod(2027)$
$990 = 2^{1819} \bmod(2027)$	$1040 = 2^{1831} \bmod(2027)$	$1090 = 2^{193} \bmod(2027)$
$991 = 2^{1519} \bmod(2027)$	$1041 = 2^{1253} \bmod(2027)$	$1091 = 2^{1438} \bmod(2027)$
$992 = 2^{1501} \bmod(2027)$	$1042 = 2^{1345} \bmod(2027)$	$1092 = 2^{1897} \bmod(2027)$
$993 = 2^{1106} \bmod(2027)$	$1043 = 2^{1392} \bmod(2027)$	$1093 = 2^{87} \bmod(2027)$
$994 = 2^{1152} \bmod(2027)$	$1044 = 2^{1175} \bmod(2027)$	$1094 = 2^{1735} \bmod(2027)$
$995 = 2^{1787} \bmod(2027)$	$1045 = 2^{292} \bmod(2027)$	$1095 = 2^{124} \bmod(2027)$
$996 = 2^{684} \bmod(2027)$	$1046 = 2^{1826} \bmod(2027)$	$1096 = 2^{1535} \bmod(2027)$
$997 = 2^{579} \bmod(2027)$	$1047 = 2^{416} \bmod(2027)$	$1097 = 2^{709} \bmod(2027)$
$998 = 2^{482} \bmod(2027)$	$1048 = 2^{262} \bmod(2027)$	$1098 = 2^{1741} \bmod(2027)$
$999 = 2^{1621} \bmod(2027)$	$1049 = 2^{1421} \bmod(2027)$	$1099 = 2^{1627} \bmod(2027)$
$1000 = 2^{1858} \bmod(2027)$	$1050 = 2^{1924} \bmod(2027)$	$1100 = 2^{1199} \bmod(2027)$
$1001 = 2^{898} \bmod(2027)$	$1051 = 2^{167} \bmod(2027)$	$1101 = 2^{1640} \bmod(2027)$
$1002 = 2^{993} \bmod(2027)$	$1052 = 2^{1039} \bmod(2027)$	$1102 = 2^{1674} \bmod(2027)$
$1003 = 2^{1023} \bmod(2027)$	$1053 = 2^{986} \bmod(2027)$	$1103 = 2^{311} \bmod(2027)$
$1004 = 2^{50} \bmod(2027)$	$1054 = 2^{1127} \bmod(2027)$	$1104 = 2^{267} \bmod(2027)$
$1005 = 2^{642} \bmod(2027)$	$1055 = 2^{399} \bmod(2027)$	$1105 = 2^{1457} \bmod(2027)$
$1006 = 2^{1237} \bmod(2027)$	$1056 = 2^{1598} \bmod(2027)$	$1106 = 2^{717} \bmod(2027)$
$1007 = 2^{870} \bmod(2027)$	$1057 = 2^{890} \bmod(2027)$	$1107 = 2^{940} \bmod(2027)$
$1008 = 2^{297} \bmod(2027)$	$1058 = 2^{1989} \bmod(2027)$	$1108 = 2^{574} \bmod(2027)$
$1009 = 2^{1576} \bmod(2027)$	$1059 = 2^{1612} \bmod(2027)$	$1109 = 2^{1490} \bmod(2027)$
$1010 = 2^{741} \bmod(2027)$	$1060 = 2^{1777} \bmod(2027)$	$1110 = 2^{1001} \bmod(2027)$
$1011 = 2^{955} \bmod(2027)$	$1061 = 2^{1006} \bmod(2027)$	$1111 = 2^{82} \bmod(2027)$
$1012 = 2^{1294} \bmod(2027)$	$1062 = 2^{1958} \bmod(2027)$	$1112 = 2^{388} \bmod(2027)$
$1013 = 2^{1012} \bmod(2027)$	$1063 = 2^{1874} \bmod(2027)$	$1113 = 2^{1843} \bmod(2027)$

$1114 = 2^{698} \bmod(2027)$	$1164 = 2^{217} \bmod(2027)$	$1214 = 2^{355} \bmod(2027)$
$1115 = 2^{337} \bmod(2027)$	$1165 = 2^{1078} \bmod(2027)$	$1215 = 2^{1353} \bmod(2027)$
$1116 = 2^{36} \bmod(2027)$	$1166 = 2^{1118} \bmod(2027)$	$1216 = 2^{1070} \bmod(2027)$
$1117 = 2^{544} \bmod(2027)$	$1167 = 2^{1447} \bmod(2027)$	$1217 = 2^{59} \bmod(2027)$
$1118 = 2^{348} \bmod(2027)$	$1168 = 2^{1929} \bmod(2027)$	$1218 = 2^{621} \bmod(2027)$
$1119 = 2^{455} \bmod(2027)$	$1169 = 2^{439} \bmod(2027)$	$1219 = 2^{1813} \bmod(2027)$
$1120 = 2^{1703} \bmod(2027)$	$1170 = 2^{366} \bmod(2027)$	$1220 = 2^{1121} \bmod(2027)$
$1121 = 2^{431} \bmod(2027)$	$1171 = 2^{235} \bmod(2027)$	$1221 = 2^{342} \bmod(2027)$
$1122 = 2^{1224} \bmod(2027)$	$1172 = 2^{558} \bmod(2027)$	$1222 = 2^{666} \bmod(2027)$
$1123 = 2^{180} \bmod(2027)$	$1173 = 2^{1919} \bmod(2027)$	$1223 = 2^{1714} \bmod(2027)$
$1124 = 2^{1513} \bmod(2027)$	$1174 = 2^{1526} \bmod(2027)$	$1224 = 2^{197} \bmod(2027)$
$1125 = 2^{393} \bmod(2027)$	$1175 = 2^{693} \bmod(2027)$	$1225 = 2^{1370} \bmod(2027)$
$1126 = 2^{449} \bmod(2027)$	$1176 = 2^{1769} \bmod(2027)$	$1226 = 2^{1541} \bmod(2027)$
$1127 = 2^{1465} \bmod(2027)$	$1177 = 2^{530} \bmod(2027)$	$1227 = 2^{904} \bmod(2027)$
$1128 = 2^{1092} \bmod(2027)$	$1178 = 2^{535} \bmod(2027)$	$1228 = 2^{1450} \bmod(2027)$
$1129 = 2^{1321} \bmod(2027)$	$1179 = 2^{823} \bmod(2027)$	$1229 = 2^{63} \bmod(2027)$
$1130 = 2^{1134} \bmod(2027)$	$1180 = 2^{1338} \bmod(2027)$	$1230 = 2^{320} \bmod(2027)$
$1131 = 2^{749} \bmod(2027)$	$1181 = 2^{359} \bmod(2027)$	$1231 = 2^{833} \bmod(2027)$
$1132 = 2^{1268} \bmod(2027)$	$1182 = 2^{672} \bmod(2027)$	$1232 = 2^{1044} \bmod(2027)$
$1133 = 2^{933} \bmod(2027)$	$1183 = 2^{1471} \bmod(2027)$	$1233 = 2^{70} \bmod(2027)$
$1134 = 2^{858} \bmod(2027)$	$1184 = 2^{780} \bmod(2027)$	$1234 = 2^{21} \bmod(2027)$
$1135 = 2^{1409} \bmod(2027)$	$1185 = 2^{1212} \bmod(2027)$	$1235 = 2^{865} \bmod(2027)$
$1136 = 2^{1426} \bmod(2027)$	$1186 = 2^{205} \bmod(2027)$	$1236 = 2^{1932} \bmod(2027)$
$1137 = 2^{921} \bmod(2027)$	$1187 = 2^{970} \bmod(2027)$	$1237 = 2^{1944} \bmod(2027)$
$1138 = 2^{681} \bmod(2027)$	$1188 = 2^{133} \bmod(2027)$	$1238 = 2^{306} \bmod(2027)$
$1139 = 2^{47} \bmod(2027)$	$1189 = 2^{703} \bmod(2027)$	$1239 = 2^{1404} \bmod(2027)$
$1140 = 2^{1291} \bmod(2027)$	$1190 = 2^{1329} \bmod(2027)$	$1240 = 2^{1442} \bmod(2027)$
$1141 = 2^{1880} \bmod(2027)$	$1191 = 2^{1364} \bmod(2027)$	$1241 = 2^{1555} \bmod(2027)$
$1142 = 2^{605} \bmod(2027)$	$1192 = 2^{1666} \bmod(2027)$	$1242 = 2^{828} \bmod(2027)$
$1143 = 2^{503} \bmod(2027)$	$1193 = 2^{1681} \bmod(2027)$	$1243 = 2^{475} \bmod(2027)$
$1144 = 2^{1172} \bmod(2027)$	$1194 = 2^{101} \bmod(2027)$	$1244 = 2^{442} \bmod(2027)$
$1145 = 2^{1036} \bmod(2027)$	$1195 = 2^{877} \bmod(2027)$	$1245 = 2^{625} \bmod(2027)$
$1146 = 2^{1774} \bmod(2027)$	$1196 = 2^{1867} \bmod(2027)$	$1246 = 2^{1720} \bmod(2027)$
$1147 = 2^{245} \bmod(2027)$	$1197 = 2^{1357} \bmod(2027)$	$1247 = 2^{1098} \bmod(2027)$
$1148 = 2^{1851} \bmod(2027)$	$1198 = 2^{657} \bmod(2027)$	$1248 = 2^{145} \bmod(2027)$
$1149 = 2^{1085} \bmod(2027)$	$1199 = 2^{1560} \bmod(2027)$	$1249 = 2^{153} \bmod(2027)$
$1150 = 2^{1894} \bmod(2027)$	$1200 = 2^{172} \bmod(2027)$	$1250 = 2^{1799} \bmod(2027)$
$1151 = 2^{1196} \bmod(2027)$	$1201 = 2^{110} \bmod(2027)$	$1251 = 2^{949} \bmod(2027)$
$1152 = 2^{571} \bmod(2027)$	$1202 = 2^{466} \bmod(2027)$	$1252 = 2^{369} \bmod(2027)$
$1153 = 2^{33} \bmod(2027)$	$1203 = 2^{638} \bmod(2027)$	$1253 = 2^{41} \bmod(2027)$
$1154 = 2^{1510} \bmod(2027)$	$1204 = 2^{220} \bmod(2027)$	$1254 = 2^{632} \bmod(2027)$
$1155 = 2^{1265} \bmod(2027)$	$1205 = 2^{802} \bmod(2027)$	$1255 = 2^{2017} \bmod(2027)$
$1156 = 2^{1288} \bmod(2027)$	$1206 = 2^{982} \bmod(2027)$	$1256 = 2^{1901} \bmod(2027)$
$1157 = 2^{1848} \bmod(2027)$	$1207 = 2^{1052} \bmod(2027)$	$1257 = 2^{1997} \bmod(2027)$
$1158 = 2^{1285} \bmod(2027)$	$1208 = 2^{1164} \bmod(2027)$	$1258 = 2^{406} \bmod(2027)$
$1159 = 2^{214} \bmod(2027)$	$1209 = 2^{1636} \bmod(2027)$	$1259 = 2^{1303} \bmod(2027)$
$1160 = 2^{555} \bmod(2027)$	$1210 = 2^{540} \bmod(2027)$	$1260 = 2^{238} \bmod(2027)$
$1161 = 2^{1335} \bmod(2027)$	$1211 = 2^{929} \bmod(2027)$	$1261 = 2^{1817} \bmod(2027)$
$1162 = 2^{130} \bmod(2027)$	$1212 = 2^{1081} \bmod(2027)$	$1262 = 2^{1150} \bmod(2027)$
$1163 = 2^{1864} \bmod(2027)$	$1213 = 2^{1074} \bmod(2027)$	$1263 = 2^{480} \bmod(2027)$

$1264 = 2^{991} \bmod(2027)$	$1314 = 2^{464} \bmod(2027)$	$1364 = 2^{783} \bmod(2027)$
$1265 = 2^{1235} \bmod(2027)$	$1315 = 2^{980} \bmod(2027)$	$1365 = 2^{1838} \bmod(2027)$
$1266 = 2^{739} \bmod(2027)$	$1316 = 2^{538} \bmod(2027)$	$1366 = 2^{1031} \bmod(2027)$
$1267 = 2^{2023} \bmod(2027)$	$1317 = 2^{353} \bmod(2027)$	$1367 = 2^{525} \bmod(2027)$
$1268 = 2^{561} \bmod(2027)$	$1318 = 2^{619} \bmod(2027)$	$1368 = 2^{1631} \bmod(2027)$
$1269 = 2^{1653} \bmod(2027)$	$1319 = 2^{664} \bmod(2027)$	$1369 = 2^{1550} \bmod(2027)$
$1270 = 2^{1909} \bmod(2027)$	$1320 = 2^{1539} \bmod(2027)$	$1370 = 2^{1476} \bmod(2027)$
$1271 = 2^{1590} \bmod(2027)$	$1321 = 2^{318} \bmod(2027)$	$1371 = 2^{1111} \bmod(2027)$
$1272 = 2^{91} \bmod(2027)$	$1322 = 2^{19} \bmod(2027)$	$1372 = 2^{1215} \bmod(2027)$
$1273 = 2^{1481} \bmod(2027)$	$1323 = 2^{304} \bmod(2027)$	$1373 = 2^{1545} \bmod(2027)$
$1274 = 2^{1343} \bmod(2027)$	$1324 = 2^{826} \bmod(2027)$	$1374 = 2^{1376} \bmod(2027)$
$1275 = 2^{1824} \bmod(2027)$	$1325 = 2^{1718} \bmod(2027)$	$1375 = 2^{1140} \bmod(2027)$
$1276 = 2^{1922} \bmod(2027)$	$1326 = 2^{1797} \bmod(2027)$	$1376 = 2^{494} \bmod(2027)$
$1277 = 2^{1125} \bmod(2027)$	$1327 = 2^{630} \bmod(2027)$	$1377 = 2^{758} \bmod(2027)$
$1278 = 2^{1987} \bmod(2027)$	$1328 = 2^{404} \bmod(2027)$	$1378 = 2^{1691} \bmod(2027)$
$1279 = 2^{1956} \bmod(2027)$	$1329 = 2^{1148} \bmod(2027)$	$1379 = 2^{118} \bmod(2027)$
$1280 = 2^{1977} \bmod(2027)$	$1330 = 2^{737} \bmod(2027)$	$1380 = 2^{208} \bmod(2027)$
$1281 = 2^{1187} \bmod(2027)$	$1331 = 2^{1907} \bmod(2027)$	$1381 = 2^{1708} \bmod(2027)$
$1282 = 2^{593} \bmod(2027)$	$1332 = 2^{1341} \bmod(2027)$	$1382 = 2^{1727} \bmod(2027)$
$1283 = 2^{768} \bmod(2027)$	$1333 = 2^{1985} \bmod(2027)$	$1383 = 2^{725} \bmod(2027)$
$1284 = 2^{1529} \bmod(2027)$	$1334 = 2^{591} \bmod(2027)$	$1384 = 2^{1203} \bmod(2027)$
$1285 = 2^{549} \bmod(2027)$	$1335 = 2^{189} \bmod(2027)$	$1385 = 2^{515} \bmod(2027)$
$1286 = 2^{191} \bmod(2027)$	$1336 = 2^{713} \bmod(2027)$	$1386 = 2^{1605} \bmod(2027)$
$1287 = 2^{1733} \bmod(2027)$	$1337 = 2^{1220} \bmod(2027)$	$1387 = 2^{963} \bmod(2027)$
$1288 = 2^{1739} \bmod(2027)$	$1338 = 2^{677} \bmod(2027)$	$1388 = 2^{973} \bmod(2027)$
$1289 = 2^{1672} \bmod(2027)$	$1339 = 2^{1506} \bmod(2027)$	$1389 = 2^{908} \bmod(2027)$
$1290 = 2^{715} \bmod(2027)$	$1340 = 2^{362} \bmod(2027)$	$1390 = 2^{329} \bmod(2027)$
$1291 = 2^{999} \bmod(2027)$	$1341 = 2^{201} \bmod(2027)$	$1391 = 2^{1103} \bmod(2027)$
$1292 = 2^{696} \bmod(2027)$	$1342 = 2^{462} \bmod(2027)$	$1392 = 2^{895} \bmod(2027)$
$1293 = 2^{346} \bmod(2027)$	$1343 = 2^{617} \bmod(2027)$	$1393 = 2^{1573} \bmod(2027)$
$1294 = 2^{1222} \bmod(2027)$	$1344 = 2^{17} \bmod(2027)$	$1394 = 2^{1751} \bmod(2027)$
$1295 = 2^{447} \bmod(2027)$	$1345 = 2^{1795} \bmod(2027)$	$1395 = 2^{2003} \bmod(2027)$
$1296 = 2^{1132} \bmod(2027)$	$1346 = 2^{735} \bmod(2027)$	$1396 = 2^{136} \bmod(2027)$
$1297 = 2^{856} \bmod(2027)$	$1347 = 2^{589} \bmod(2027)$	$1397 = 2^{1250} \bmod(2027)$
$1298 = 2^{679} \bmod(2027)$	$1348 = 2^{675} \bmod(2027)$	$1398 = 2^{1418} \bmod(2027)$
$1299 = 2^{603} \bmod(2027)$	$1349 = 2^{460} \bmod(2027)$	$1399 = 2^{887} \bmod(2027)$
$1300 = 2^{1772} \bmod(2027)$	$1350 = 2^{733} \bmod(2027)$	$1400 = 2^{1644} \bmod(2027)$
$1301 = 2^{1892} \bmod(2027)$	$1351 = 2^{731} \bmod(2027)$	$1401 = 2^{1381} \bmod(2027)$
$1302 = 2^{1508} \bmod(2027)$	$1352 = 2^{1745} \bmod(2027)$	$1402 = 2^{785} \bmod(2027)$
$1303 = 2^{1283} \bmod(2027)$	$1353 = 2^{1687} \bmod(2027)$	$1403 = 2^{1157} \bmod(2027)$
$1304 = 2^{128} \bmod(2027)$	$1354 = 2^{1747} \bmod(2027)$	$1404 = 2^{706} \bmod(2027)$
$1305 = 2^{1116} \bmod(2027)$	$1355 = 2^{1029} \bmod(2027)$	$1405 = 2^{1454} \bmod(2027)$
$1306 = 2^{364} \bmod(2027)$	$1356 = 2^{1474} \bmod(2027)$	$1406 = 2^{1840} \bmod(2027)$
$1307 = 2^{1524} \bmod(2027)$	$1357 = 2^{1374} \bmod(2027)$	$1407 = 2^{428} \bmod(2027)$
$1308 = 2^{533} \bmod(2027)$	$1358 = 2^{1689} \bmod(2027)$	$1408 = 2^{1318} \bmod(2027)$
$1309 = 2^{670} \bmod(2027)$	$1359 = 2^{1725} \bmod(2027)$	$1409 = 2^{918} \bmod(2027)$
$1310 = 2^{203} \bmod(2027)$	$1360 = 2^{1603} \bmod(2027)$	$1410 = 2^{1033} \bmod(2027)$
$1311 = 2^{1327} \bmod(2027)$	$1361 = 2^{327} \bmod(2027)$	$1411 = 2^{30} \bmod(2027)$
$1312 = 2^{99} \bmod(2027)$	$1362 = 2^{1749} \bmod(2027)$	$1412 = 2^{1332} \bmod(2027)$
$1313 = 2^{655} \bmod(2027)$	$1363 = 2^{1416} \bmod(2027)$	$1413 = 2^{436} \bmod(2027)$

$1414 = 2^{527} \bmod(2027)$	$1464 = 2^{1461} \bmod(2027)$	$1514 = 2^{897} \bmod(2027)$
$1415 = 2^{1209} \bmod(2027)$	$1465 = 2^{499} \bmod(2027)$	$1515 = 2^{1022} \bmod(2027)$
$1416 = 2^{1678} \bmod(2027)$	$1466 = 2^{210} \bmod(2027)$	$1516 = 2^{641} \bmod(2027)$
$1417 = 2^{107} \bmod(2027)$	$1467 = 2^{689} \bmod(2027)$	$1517 = 2^{869} \bmod(2027)$
$1418 = 2^{1633} \bmod(2027)$	$1468 = 2^{1360} \bmod(2027)$	$1518 = 2^{1575} \bmod(2027)$
$1419 = 2^{56} \bmod(2027)$	$1469 = 2^{1048} \bmod(2027)$	$1519 = 2^{954} \bmod(2027)$
$1420 = 2^{1367} \bmod(2027)$	$1470 = 2^{1710} \bmod(2027)$	$1520 = 2^{1011} \bmod(2027)$
$1421 = 2^{67} \bmod(2027)$	$1471 = 2^{1400} \bmod(2027)$	$1521 = 2^{280} \bmod(2027)$
$1422 = 2^{1552} \bmod(2027)$	$1472 = 2^{2013} \bmod(2027)$	$1522 = 2^{1753} \bmod(2027)$
$1423 = 2^{150} \bmod(2027)$	$1473 = 2^{1586} \bmod(2027)$	$1523 = 2^{1309} \bmod(2027)$
$1424 = 2^{1994} \bmod(2027)$	$1474 = 2^{1729} \bmod(2027)$	$1524 = 2^{223} \bmod(2027)$
$1425 = 2^{1232} \bmod(2027)$	$1475 = 2^{1279} \bmod(2027)$	$1525 = 2^{1062} \bmod(2027)$
$1426 = 2^{1478} \bmod(2027)$	$1476 = 2^{660} \bmod(2027)$	$1526 = 2^{2005} \bmod(2027)$
$1427 = 2^{1184} \bmod(2027)$	$1477 = 2^{185} \bmod(2027)$	$1527 = 2^{844} \bmod(2027)$
$1428 = 2^{1669} \bmod(2027)$	$1478 = 2^{727} \bmod(2027)$	$1528 = 2^{1494} \bmod(2027)$
$1429 = 2^{853} \bmod(2027)$	$1479 = 2^{521} \bmod(2027)$	$1529 = 2^{1696} \bmod(2027)$
$1430 = 2^{1113} \bmod(2027)$	$1480 = 2^{721} \bmod(2027)$	$1530 = 2^{138} \bmod(2027)$
$1431 = 2^{652} \bmod(2027)$	$1481 = 2^{883} \bmod(2027)$	$1531 = 2^{487} \bmod(2027)$
$1432 = 2^{315} \bmod(2027)$	$1482 = 2^{1205} \bmod(2027)$	$1532 = 2^{805} \bmod(2027)$
$1433 = 2^{1145} \bmod(2027)$	$1483 = 2^{648} \bmod(2027)$	$1533 = 2^{1936} \bmod(2027)$
$1434 = 2^{1217} \bmod(2027)$	$1484 = 2^{1563} \bmod(2027)$	$1534 = 2^{1252} \bmod(2027)$
$1435 = 2^{1792} \bmod(2027)$	$1485 = 2^{74} \bmod(2027)$	$1535 = 2^{1391} \bmod(2027)$
$1436 = 2^{1684} \bmod(2027)$	$1486 = 2^{517} \bmod(2027)$	$1536 = 2^{291} \bmod(2027)$
$1437 = 2^{324} \bmod(2027)$	$1487 = 2^{1804} \bmod(2027)$	$1537 = 2^{415} \bmod(2027)$
$1438 = 2^{1547} \bmod(2027)$	$1488 = 2^{1782} \bmod(2027)$	$1538 = 2^{1420} \bmod(2027)$
$1439 = 2^{755} \bmod(2027)$	$1489 = 2^{840} \bmod(2027)$	$1539 = 2^{166} \bmod(2027)$
$1440 = 2^{512} \bmod(2027)$	$1490 = 2^{1607} \bmod(2027)$	$1540 = 2^{985} \bmod(2027)$
$1441 = 2^{1570} \bmod(2027)$	$1491 = 2^{1433} \bmod(2027)$	$1541 = 2^{398} \bmod(2027)$
$1442 = 2^{1378} \bmod(2027)$	$1492 = 2^{175} \bmod(2027)$	$1542 = 2^{889} \bmod(2027)$
$1443 = 2^{915} \bmod(2027)$	$1493 = 2^{1260} \bmod(2027)$	$1543 = 2^{1611} \bmod(2027)$
$1444 = 2^{104} \bmod(2027)$	$1494 = 2^{965} \bmod(2027)$	$1544 = 2^{1005} \bmod(2027)$
$1445 = 2^{1229} \bmod(2027)$	$1495 = 2^{1808} \bmod(2027)$	$1545 = 2^{1873} \bmod(2027)$
$1446 = 2^{1142} \bmod(2027)$	$1496 = 2^{944} \bmod(2027)$	$1546 = 2^{1646} \bmod(2027)$
$1447 = 2^{1567} \bmod(2027)$	$1497 = 2^{763} \bmod(2027)$	$1547 = 2^{1243} \bmod(2027)$
$1448 = 2^{271} \bmod(2027)$	$1498 = 2^{975} \bmod(2027)$	$1548 = 2^{1055} \bmod(2027)$
$1449 = 2^{274} \bmod(2027)$	$1499 = 2^{584} \bmod(2027)$	$1549 = 2^{1948} \bmod(2027)$
$1450 = 2^{496} \bmod(2027)$	$1500 = 2^{113} \bmod(2027)$	$1550 = 2^{1383} \bmod(2027)$
$1451 = 2^{1583} \bmod(2027)$	$1501 = 2^{25} \bmod(2027)$	$1551 = 2^{374} \bmod(2027)$
$1452 = 2^{880} \bmod(2027)$	$1502 = 2^{910} \bmod(2027)$	$1552 = 2^{1963} \bmod(2027)$
$1453 = 2^{837} \bmod(2027)$	$1503 = 2^{1274} \bmod(2027)$	$1553 = 2^{257} \bmod(2027)$
$1454 = 2^{760} \bmod(2027)$	$1504 = 2^{812} \bmod(2027)$	$1554 = 2^{787} \bmod(2027)$
$1455 = 2^{158} \bmod(2027)$	$1505 = 2^{161} \bmod(2027)$	$1555 = 2^{383} \bmod(2027)$
$1456 = 2^{1617} \bmod(2027)$	$1506 = 2^{331} \bmod(2027)$	$1556 = 2^{1167} \bmod(2027)$
$1457 = 2^{277} \bmod(2027)$	$1507 = 2^{817} \bmod(2027)$	$1557 = 2^{1764} \bmod(2027)$
$1458 = 2^{1693} \bmod(2027)$	$1508 = 2^{469} \bmod(2027)$	$1558 = 2^{1159} \bmod(2027)$
$1459 = 2^{412} \bmod(2027)$	$1509 = 2^{1518} \bmod(2027)$	$1559 = 2^{1437} \bmod(2027)$
$1460 = 2^{1870} \bmod(2027)$	$1510 = 2^{1105} \bmod(2027)$	$1560 = 2^{86} \bmod(2027)$
$1461 = 2^{254} \bmod(2027)$	$1511 = 2^{1786} \bmod(2027)$	$1561 = 2^{123} \bmod(2027)$
$1462 = 2^{120} \bmod(2027)$	$1512 = 2^{578} \bmod(2027)$	$1562 = 2^{708} \bmod(2027)$
$1463 = 2^{78} \bmod(2027)$	$1513 = 2^{1620} \bmod(2027)$	$1563 = 2^{1626} \bmod(2027)$

$1564 = 2^{1639} \bmod(2027)$	$1614 = 2^{109} \bmod(2027)$	$1664 = 2^{1891} \bmod(2027)$
$1565 = 2^{310} \bmod(2027)$	$1615 = 2^{637} \bmod(2027)$	$1665 = 2^{1282} \bmod(2027)$
$1566 = 2^{1456} \bmod(2027)$	$1616 = 2^{801} \bmod(2027)$	$1666 = 2^{1115} \bmod(2027)$
$1567 = 2^{939} \bmod(2027)$	$1617 = 2^{1051} \bmod(2027)$	$1667 = 2^{1523} \bmod(2027)$
$1568 = 2^{1489} \bmod(2027)$	$1618 = 2^{1635} \bmod(2027)$	$1668 = 2^{669} \bmod(2027)$
$1569 = 2^{81} \bmod(2027)$	$1619 = 2^{928} \bmod(2027)$	$1669 = 2^{1326} \bmod(2027)$
$1570 = 2^{1842} \bmod(2027)$	$1620 = 2^{1073} \bmod(2027)$	$1670 = 2^{654} \bmod(2027)$
$1571 = 2^{336} \bmod(2027)$	$1621 = 2^{1352} \bmod(2027)$	$1671 = 2^{979} \bmod(2027)$
$1572 = 2^{543} \bmod(2027)$	$1622 = 2^{58} \bmod(2027)$	$1672 = 2^{352} \bmod(2027)$
$1573 = 2^{454} \bmod(2027)$	$1623 = 2^{1812} \bmod(2027)$	$1673 = 2^{663} \bmod(2027)$
$1574 = 2^{430} \bmod(2027)$	$1624 = 2^{341} \bmod(2027)$	$1674 = 2^{317} \bmod(2027)$
$1575 = 2^{179} \bmod(2027)$	$1625 = 2^{1713} \bmod(2027)$	$1675 = 2^{303} \bmod(2027)$
$1576 = 2^{392} \bmod(2027)$	$1626 = 2^{1369} \bmod(2027)$	$1676 = 2^{1717} \bmod(2027)$
$1577 = 2^{1464} \bmod(2027)$	$1627 = 2^{903} \bmod(2027)$	$1677 = 2^{629} \bmod(2027)$
$1578 = 2^{1320} \bmod(2027)$	$1628 = 2^{62} \bmod(2027)$	$1678 = 2^{1147} \bmod(2027)$
$1579 = 2^{748} \bmod(2027)$	$1629 = 2^{832} \bmod(2027)$	$1679 = 2^{1906} \bmod(2027)$
$1580 = 2^{932} \bmod(2027)$	$1630 = 2^{69} \bmod(2027)$	$1680 = 2^{1984} \bmod(2027)$
$1581 = 2^{1408} \bmod(2027)$	$1631 = 2^{864} \bmod(2027)$	$1681 = 2^{188} \bmod(2027)$
$1582 = 2^{920} \bmod(2027)$	$1632 = 2^{1943} \bmod(2027)$	$1682 = 2^{1219} \bmod(2027)$
$1583 = 2^{46} \bmod(2027)$	$1633 = 2^{1403} \bmod(2027)$	$1683 = 2^{1505} \bmod(2027)$
$1584 = 2^{1879} \bmod(2027)$	$1634 = 2^{1554} \bmod(2027)$	$1684 = 2^{200} \bmod(2027)$
$1585 = 2^{502} \bmod(2027)$	$1635 = 2^{474} \bmod(2027)$	$1685 = 2^{616} \bmod(2027)$
$1586 = 2^{1035} \bmod(2027)$	$1636 = 2^{624} \bmod(2027)$	$1686 = 2^{1794} \bmod(2027)$
$1587 = 2^{244} \bmod(2027)$	$1637 = 2^{1097} \bmod(2027)$	$1687 = 2^{588} \bmod(2027)$
$1588 = 2^{1084} \bmod(2027)$	$1638 = 2^{152} \bmod(2027)$	$1688 = 2^{459} \bmod(2027)$
$1589 = 2^{1195} \bmod(2027)$	$1639 = 2^{948} \bmod(2027)$	$1689 = 2^{730} \bmod(2027)$
$1590 = 2^{32} \bmod(2027)$	$1640 = 2^{40} \bmod(2027)$	$1690 = 2^{1686} \bmod(2027)$
$1591 = 2^{1264} \bmod(2027)$	$1641 = 2^{2016} \bmod(2027)$	$1691 = 2^{1028} \bmod(2027)$
$1592 = 2^{1847} \bmod(2027)$	$1642 = 2^{1996} \bmod(2027)$	$1692 = 2^{1373} \bmod(2027)$
$1593 = 2^{213} \bmod(2027)$	$1643 = 2^{1302} \bmod(2027)$	$1693 = 2^{1724} \bmod(2027)$
$1594 = 2^{1334} \bmod(2027)$	$1644 = 2^{1816} \bmod(2027)$	$1694 = 2^{326} \bmod(2027)$
$1595 = 2^{1863} \bmod(2027)$	$1645 = 2^{479} \bmod(2027)$	$1695 = 2^{1415} \bmod(2027)$
$1596 = 2^{1077} \bmod(2027)$	$1646 = 2^{1234} \bmod(2027)$	$1696 = 2^{1837} \bmod(2027)$
$1597 = 2^{1446} \bmod(2027)$	$1647 = 2^{2022} \bmod(2027)$	$1697 = 2^{524} \bmod(2027)$
$1598 = 2^{438} \bmod(2027)$	$1648 = 2^{1652} \bmod(2027)$	$1698 = 2^{1549} \bmod(2027)$
$1599 = 2^{234} \bmod(2027)$	$1649 = 2^{1589} \bmod(2027)$	$1699 = 2^{1110} \bmod(2027)$
$1600 = 2^{1918} \bmod(2027)$	$1650 = 2^{1480} \bmod(2027)$	$1700 = 2^{1544} \bmod(2027)$
$1601 = 2^{692} \bmod(2027)$	$1651 = 2^{1823} \bmod(2027)$	$1701 = 2^{1139} \bmod(2027)$
$1602 = 2^{529} \bmod(2027)$	$1652 = 2^{1124} \bmod(2027)$	$1702 = 2^{757} \bmod(2027)$
$1603 = 2^{822} \bmod(2027)$	$1653 = 2^{1955} \bmod(2027)$	$1703 = 2^{117} \bmod(2027)$
$1604 = 2^{358} \bmod(2027)$	$1654 = 2^{1186} \bmod(2027)$	$1704 = 2^{1707} \bmod(2027)$
$1605 = 2^{1470} \bmod(2027)$	$1655 = 2^{767} \bmod(2027)$	$1705 = 2^{724} \bmod(2027)$
$1606 = 2^{1211} \bmod(2027)$	$1656 = 2^{548} \bmod(2027)$	$1706 = 2^{514} \bmod(2027)$
$1607 = 2^{969} \bmod(2027)$	$1657 = 2^{1732} \bmod(2027)$	$1707 = 2^{962} \bmod(2027)$
$1608 = 2^{702} \bmod(2027)$	$1658 = 2^{1671} \bmod(2027)$	$1708 = 2^{907} \bmod(2027)$
$1609 = 2^{1363} \bmod(2027)$	$1659 = 2^{998} \bmod(2027)$	$1709 = 2^{1102} \bmod(2027)$
$1610 = 2^{1680} \bmod(2027)$	$1660 = 2^{345} \bmod(2027)$	$1710 = 2^{1572} \bmod(2027)$
$1611 = 2^{876} \bmod(2027)$	$1661 = 2^{446} \bmod(2027)$	$1711 = 2^{2002} \bmod(2027)$
$1612 = 2^{1356} \bmod(2027)$	$1662 = 2^{855} \bmod(2027)$	$1712 = 2^{1249} \bmod(2027)$
$1613 = 2^{1559} \bmod(2027)$	$1663 = 2^{602} \bmod(2027)$	$1713 = 2^{886} \bmod(2027)$

$1714 = 2^{1380} \bmod(2027)$	$1764 = 2^{24} \bmod(2027)$	$1814 = 2^{691} \bmod(2027)$
$1715 = 2^{1156} \bmod(2027)$	$1765 = 2^{1273} \bmod(2027)$	$1815 = 2^{821} \bmod(2027)$
$1716 = 2^{1453} \bmod(2027)$	$1766 = 2^{160} \bmod(2027)$	$1816 = 2^{1469} \bmod(2027)$
$1717 = 2^{427} \bmod(2027)$	$1767 = 2^{816} \bmod(2027)$	$1817 = 2^{968} \bmod(2027)$
$1718 = 2^{917} \bmod(2027)$	$1768 = 2^{1517} \bmod(2027)$	$1818 = 2^{1362} \bmod(2027)$
$1719 = 2^{29} \bmod(2027)$	$1769 = 2^{1785} \bmod(2027)$	$1819 = 2^{875} \bmod(2027)$
$1720 = 2^{435} \bmod(2027)$	$1770 = 2^{1619} \bmod(2027)$	$1820 = 2^{1558} \bmod(2027)$
$1721 = 2^{1208} \bmod(2027)$	$1771 = 2^{1021} \bmod(2027)$	$1821 = 2^{636} \bmod(2027)$
$1722 = 2^{106} \bmod(2027)$	$1772 = 2^{868} \bmod(2027)$	$1822 = 2^{1050} \bmod(2027)$
$1723 = 2^{55} \bmod(2027)$	$1773 = 2^{953} \bmod(2027)$	$1823 = 2^{927} \bmod(2027)$
$1724 = 2^{66} \bmod(2027)$	$1774 = 2^{279} \bmod(2027)$	$1824 = 2^{1351} \bmod(2027)$
$1725 = 2^{149} \bmod(2027)$	$1775 = 2^{1308} \bmod(2027)$	$1825 = 2^{1811} \bmod(2027)$
$1726 = 2^{1231} \bmod(2027)$	$1776 = 2^{1061} \bmod(2027)$	$1826 = 2^{1712} \bmod(2027)$
$1727 = 2^{1183} \bmod(2027)$	$1777 = 2^{843} \bmod(2027)$	$1827 = 2^{902} \bmod(2027)$
$1728 = 2^{852} \bmod(2027)$	$1778 = 2^{1695} \bmod(2027)$	$1828 = 2^{831} \bmod(2027)$
$1729 = 2^{651} \bmod(2027)$	$1779 = 2^{486} \bmod(2027)$	$1829 = 2^{863} \bmod(2027)$
$1730 = 2^{1144} \bmod(2027)$	$1780 = 2^{1935} \bmod(2027)$	$1830 = 2^{1402} \bmod(2027)$
$1731 = 2^{1791} \bmod(2027)$	$1781 = 2^{1390} \bmod(2027)$	$1831 = 2^{473} \bmod(2027)$
$1732 = 2^{323} \bmod(2027)$	$1782 = 2^{414} \bmod(2027)$	$1832 = 2^{1096} \bmod(2027)$
$1733 = 2^{754} \bmod(2027)$	$1783 = 2^{165} \bmod(2027)$	$1833 = 2^{947} \bmod(2027)$
$1734 = 2^{1569} \bmod(2027)$	$1784 = 2^{397} \bmod(2027)$	$1834 = 2^{2015} \bmod(2027)$
$1735 = 2^{914} \bmod(2027)$	$1785 = 2^{1610} \bmod(2027)$	$1835 = 2^{1301} \bmod(2027)$
$1736 = 2^{1228} \bmod(2027)$	$1786 = 2^{1872} \bmod(2027)$	$1836 = 2^{478} \bmod(2027)$
$1737 = 2^{1566} \bmod(2027)$	$1787 = 2^{1242} \bmod(2027)$	$1837 = 2^{2021} \bmod(2027)$
$1738 = 2^{273} \bmod(2027)$	$1788 = 2^{1947} \bmod(2027)$	$1838 = 2^{1588} \bmod(2027)$
$1739 = 2^{1582} \bmod(2027)$	$1789 = 2^{373} \bmod(2027)$	$1839 = 2^{1822} \bmod(2027)$
$1740 = 2^{836} \bmod(2027)$	$1790 = 2^{256} \bmod(2027)$	$1840 = 2^{1954} \bmod(2027)$
$1741 = 2^{157} \bmod(2027)$	$1791 = 2^{382} \bmod(2027)$	$1841 = 2^{766} \bmod(2027)$
$1742 = 2^{276} \bmod(2027)$	$1792 = 2^{1763} \bmod(2027)$	$1842 = 2^{1731} \bmod(2027)$
$1743 = 2^{411} \bmod(2027)$	$1793 = 2^{1436} \bmod(2027)$	$1843 = 2^{997} \bmod(2027)$
$1744 = 2^{253} \bmod(2027)$	$1794 = 2^{122} \bmod(2027)$	$1844 = 2^{445} \bmod(2027)$
$1745 = 2^{77} \bmod(2027)$	$1795 = 2^{1625} \bmod(2027)$	$1845 = 2^{601} \bmod(2027)$
$1746 = 2^{498} \bmod(2027)$	$1796 = 2^{309} \bmod(2027)$	$1846 = 2^{1281} \bmod(2027)$
$1747 = 2^{688} \bmod(2027)$	$1797 = 2^{938} \bmod(2027)$	$1847 = 2^{1522} \bmod(2027)$
$1748 = 2^{1047} \bmod(2027)$	$1798 = 2^{80} \bmod(2027)$	$1848 = 2^{1325} \bmod(2027)$
$1749 = 2^{1399} \bmod(2027)$	$1799 = 2^{335} \bmod(2027)$	$1849 = 2^{978} \bmod(2027)$
$1750 = 2^{1585} \bmod(2027)$	$1800 = 2^{453} \bmod(2027)$	$1850 = 2^{662} \bmod(2027)$
$1751 = 2^{1278} \bmod(2027)$	$1801 = 2^{178} \bmod(2027)$	$1851 = 2^{302} \bmod(2027)$
$1752 = 2^{184} \bmod(2027)$	$1802 = 2^{1463} \bmod(2027)$	$1852 = 2^{628} \bmod(2027)$
$1753 = 2^{520} \bmod(2027)$	$1803 = 2^{747} \bmod(2027)$	$1853 = 2^{1905} \bmod(2027)$
$1754 = 2^{882} \bmod(2027)$	$1804 = 2^{1407} \bmod(2027)$	$1854 = 2^{187} \bmod(2027)$
$1755 = 2^{647} \bmod(2027)$	$1805 = 2^{45} \bmod(2027)$	$1855 = 2^{1504} \bmod(2027)$
$1756 = 2^{73} \bmod(2027)$	$1806 = 2^{501} \bmod(2027)$	$1856 = 2^{615} \bmod(2027)$
$1757 = 2^{1803} \bmod(2027)$	$1807 = 2^{243} \bmod(2027)$	$1857 = 2^{587} \bmod(2027)$
$1758 = 2^{839} \bmod(2027)$	$1808 = 2^{1194} \bmod(2027)$	$1858 = 2^{729} \bmod(2027)$
$1759 = 2^{1432} \bmod(2027)$	$1809 = 2^{1263} \bmod(2027)$	$1859 = 2^{1027} \bmod(2027)$
$1760 = 2^{1259} \bmod(2027)$	$1810 = 2^{212} \bmod(2027)$	$1860 = 2^{1723} \bmod(2027)$
$1761 = 2^{1807} \bmod(2027)$	$1811 = 2^{1862} \bmod(2027)$	$1861 = 2^{1414} \bmod(2027)$
$1762 = 2^{762} \bmod(2027)$	$1812 = 2^{1445} \bmod(2027)$	$1862 = 2^{523} \bmod(2027)$
$1763 = 2^{583} \bmod(2027)$	$1813 = 2^{233} \bmod(2027)$	$1863 = 2^{1109} \bmod(2027)$

$1864 = 2^{1138} \bmod(2027)$	$1914 = 2^{177} \bmod(2027)$	$1964 = 2^{1306} \bmod(2027)$
$1865 = 2^{116} \bmod(2027)$	$1915 = 2^{746} \bmod(2027)$	$1965 = 2^{484} \bmod(2027)$
$1866 = 2^{723} \bmod(2027)$	$1916 = 2^{44} \bmod(2027)$	$1966 = 2^{163} \bmod(2027)$
$1867 = 2^{961} \bmod(2027)$	$1917 = 2^{242} \bmod(2027)$	$1967 = 2^{1240} \bmod(2027)$
$1868 = 2^{1101} \bmod(2027)$	$1918 = 2^{1262} \bmod(2027)$	$1968 = 2^{380} \bmod(2027)$
$1869 = 2^{2001} \bmod(2027)$	$1919 = 2^{1861} \bmod(2027)$	$1969 = 2^{1623} \bmod(2027)$
$1870 = 2^{885} \bmod(2027)$	$1920 = 2^{232} \bmod(2027)$	$1970 = 2^{333} \bmod(2027)$
$1871 = 2^{1155} \bmod(2027)$	$1921 = 2^{820} \bmod(2027)$	$1971 = 2^{745} \bmod(2027)$
$1872 = 2^{426} \bmod(2027)$	$1922 = 2^{967} \bmod(2027)$	$1972 = 2^{241} \bmod(2027)$
$1873 = 2^{28} \bmod(2027)$	$1923 = 2^{874} \bmod(2027)$	$1973 = 2^{1860} \bmod(2027)$
$1874 = 2^{1207} \bmod(2027)$	$1924 = 2^{635} \bmod(2027)$	$1974 = 2^{819} \bmod(2027)$
$1875 = 2^{54} \bmod(2027)$	$1925 = 2^{926} \bmod(2027)$	$1975 = 2^{873} \bmod(2027)$
$1876 = 2^{148} \bmod(2027)$	$1926 = 2^{1810} \bmod(2027)$	$1976 = 2^{925} \bmod(2027)$
$1877 = 2^{1182} \bmod(2027)$	$1927 = 2^{901} \bmod(2027)$	$1977 = 2^{900} \bmod(2027)$
$1878 = 2^{650} \bmod(2027)$	$1928 = 2^{862} \bmod(2027)$	$1978 = 2^{471} \bmod(2027)$
$1879 = 2^{1790} \bmod(2027)$	$1929 = 2^{472} \bmod(2027)$	$1979 = 2^{1299} \bmod(2027)$
$1880 = 2^{753} \bmod(2027)$	$1930 = 2^{946} \bmod(2027)$	$1980 = 2^{1820} \bmod(2027)$
$1881 = 2^{913} \bmod(2027)$	$1931 = 2^{1300} \bmod(2027)$	$1981 = 2^{995} \bmod(2027)$
$1882 = 2^{1565} \bmod(2027)$	$1932 = 2^{2020} \bmod(2027)$	$1982 = 2^{1520} \bmod(2027)$
$1883 = 2^{1581} \bmod(2027)$	$1933 = 2^{1821} \bmod(2027)$	$1983 = 2^{300} \bmod(2027)$
$1884 = 2^{156} \bmod(2027)$	$1934 = 2^{765} \bmod(2027)$	$1984 = 2^{1502} \bmod(2027)$
$1885 = 2^{410} \bmod(2027)$	$1935 = 2^{996} \bmod(2027)$	$1985 = 2^{1025} \bmod(2027)$
$1886 = 2^{76} \bmod(2027)$	$1936 = 2^{600} \bmod(2027)$	$1986 = 2^{1107} \bmod(2027)$
$1887 = 2^{687} \bmod(2027)$	$1937 = 2^{1521} \bmod(2027)$	$1987 = 2^{959} \bmod(2027)$
$1888 = 2^{1398} \bmod(2027)$	$1938 = 2^{977} \bmod(2027)$	$1988 = 2^{1153} \bmod(2027)$
$1889 = 2^{1277} \bmod(2027)$	$1939 = 2^{301} \bmod(2027)$	$1989 = 2^{52} \bmod(2027)$
$1890 = 2^{519} \bmod(2027)$	$1940 = 2^{1904} \bmod(2027)$	$1990 = 2^{1788} \bmod(2027)$
$1891 = 2^{646} \bmod(2027)$	$1941 = 2^{1503} \bmod(2027)$	$1991 = 2^{1579} \bmod(2027)$
$1892 = 2^{1802} \bmod(2027)$	$1942 = 2^{586} \bmod(2027)$	$1992 = 2^{685} \bmod(2027)$
$1893 = 2^{1431} \bmod(2027)$	$1943 = 2^{1026} \bmod(2027)$	$1993 = 2^{644} \bmod(2027)$
$1894 = 2^{1806} \bmod(2027)$	$1944 = 2^{1413} \bmod(2027)$	$1994 = 2^{580} \bmod(2027)$
$1895 = 2^{582} \bmod(2027)$	$1945 = 2^{1108} \bmod(2027)$	$1995 = 2^{1018} \bmod(2027)$
$1896 = 2^{1272} \bmod(2027)$	$1946 = 2^{115} \bmod(2027)$	$1996 = 2^{483} \bmod(2027)$
$1897 = 2^{815} \bmod(2027)$	$1947 = 2^{960} \bmod(2027)$	$1997 = 2^{1239} \bmod(2027)$
$1898 = 2^{1784} \bmod(2027)$	$1948 = 2^{2000} \bmod(2027)$	$1998 = 2^{1622} \bmod(2027)$
$1899 = 2^{1020} \bmod(2027)$	$1949 = 2^{1154} \bmod(2027)$	$1999 = 2^{744} \bmod(2027)$
$1900 = 2^{952} \bmod(2027)$	$1950 = 2^{27} \bmod(2027)$	$2000 = 2^{1859} \bmod(2027)$
$1901 = 2^{1307} \bmod(2027)$	$1951 = 2^{53} \bmod(2027)$	$2001 = 2^{872} \bmod(2027)$
$1902 = 2^{842} \bmod(2027)$	$1952 = 2^{1181} \bmod(2027)$	$2002 = 2^{899} \bmod(2027)$
$1903 = 2^{485} \bmod(2027)$	$1953 = 2^{1789} \bmod(2027)$	$2003 = 2^{1298} \bmod(2027)$
$1904 = 2^{1389} \bmod(2027)$	$1954 = 2^{912} \bmod(2027)$	$2004 = 2^{994} \bmod(2027)$
$1905 = 2^{164} \bmod(2027)$	$1955 = 2^{1580} \bmod(2027)$	$2005 = 2^{299} \bmod(2027)$
$1906 = 2^{1609} \bmod(2027)$	$1956 = 2^{409} \bmod(2027)$	$2006 = 2^{1024} \bmod(2027)$
$1907 = 2^{1241} \bmod(2027)$	$1957 = 2^{686} \bmod(2027)$	$2007 = 2^{958} \bmod(2027)$
$1908 = 2^{372} \bmod(2027)$	$1958 = 2^{1276} \bmod(2027)$	$2008 = 2^{51} \bmod(2027)$
$1909 = 2^{381} \bmod(2027)$	$1959 = 2^{645} \bmod(2027)$	$2009 = 2^{1578} \bmod(2027)$
$1910 = 2^{1435} \bmod(2027)$	$1960 = 2^{1430} \bmod(2027)$	$2010 = 2^{643} \bmod(2027)$
$1911 = 2^{1624} \bmod(2027)$	$1961 = 2^{581} \bmod(2027)$	$2011 = 2^{1017} \bmod(2027)$
$1912 = 2^{937} \bmod(2027)$	$1962 = 2^{814} \bmod(2027)$	$2012 = 2^{1238} \bmod(2027)$
$1913 = 2^{334} \bmod(2027)$	$1963 = 2^{1019} \bmod(2027)$	$2013 = 2^{743} \bmod(2027)$



$2014 = 2^{871} \bmod(2027)$	$2019 = 2^{1016} \bmod(2027)$	$2024 = 2^{1295} \bmod(2027)$
$2015 = 2^{1297} \bmod(2027)$	$2020 = 2^{742} \bmod(2027)$	$2025 = 2^{1014} \bmod(2027)$
$2016 = 2^{298} \bmod(2027)$	$2021 = 2^{1296} \bmod(2027)$	$2026 = 2^{1013} \bmod(2027)$
$2017 = 2^{957} \bmod(2027)$	$2022 = 2^{956} \bmod(2027)$	
$2018 = 2^{1577} \bmod(2027)$	$2023 = 2^{1015} \bmod(2027)$	

Por lo tanto 2 es generados de  $\mathbb{Z}_{2027}^*$

- b) Mediante el cálculo de índices encontrar  $\log_2(13) \bmod(2027)$ , tome como base  $B = \{2, 3, 5, 7, 11\}$

Tenemos la siguiente información:  $p = 2027, \alpha = 2, n = 2026, \beta = 13$ . Entonces queremos encontrar  $\log_2(13) \bmod(2027)$

- 1) Tenemos como base  $B = \{-1, 2, 3, 5, 7, 11\}$  (agregamos a  $-1$  ya que  $n$  es grande)
- 2) Buscamos las relaciones que involucren a los elementos de  $S$

$$\begin{aligned}
 2^{596} \bmod(2027) &= 121 = 11^2 \\
 2^{15} \bmod(2027) &= 336 = 2^4 \cdot 3 \cdot 7 \\
 2^{789} \bmod(2027) &= 135 = 3^3 \cdot 5 \\
 2^{1041} \bmod(2027) &= 154 = 2 \cdot 7 \cdot 11 \\
 2^{1040} \bmod(2027) &= 77 = 7 \cdot 11
 \end{aligned}$$

Con lo se genera un sistema de ecuaciones de  $5 \times 5$

$$\begin{aligned}
 15 &= 4 \log_2(2) + \log_2(3) + \log_2(7) \bmod(2026) \\
 789 &= 3 \log_2(3) + \log_2(5) \bmod(2026) \\
 1041 &= \log_2(2) + \log_2(7) + \log_2(11) \bmod(2026) \\
 1040 &= \log_2(7) + \log_2(11) \bmod(2026) \\
 586 &= 2 \log_2(11) \bmod(2026)
 \end{aligned}$$

- 3) Resolviendo el sistema de ecuaciones obtenemos:

$$\begin{aligned}
 \log_2(2) &= 1 \\
 \log_2(3) &= -731 = 1295 \\
 \log_2(5) &= 2982 = 956 \\
 \log_2(7) &= 742 \\
 \log_2(11) &= 298
 \end{aligned}$$

- 4) Elegimos  $k = 30$

Calculamos  $\beta \cdot \alpha^k = (13)(2)^{30} \bmod(2027) = 100 = 2^2 \cdot 5^2$   
 aplicando  $\log_2$  en ambos lados, tenemos:

$$\begin{aligned}
 \log_2(13) + 30 \log_2(2) &= 2 \log_2(2) + 2 \log_2(5) \bmod(2026) \\
 \log_2(13) + 30 \cdot 1 &= 2 \log_2(2) + 2 \log_2(5) \bmod(2026) \\
 \log_2(13) &= 2 \log_2(2) + 2 \log_2(5) - 30 \bmod(2026) \\
 &= (2(1) + 2(956) - 30) \bmod(2026) \\
 &= 1884 \bmod 2026 \\
 &= 1884
 \end{aligned}$$

- c) Sea el siguiente mensaje cifrado con Gammal de parámetros públicos  $gammal(n = 2027, \alpha = 2, \alpha^k = 13)$ , con base a lo previo del ejercicio dos, descifra el mensaje.

Ya que sabemos está cifrado con  $gammal$ , entonces podemos ver a cada par ordenado  $(X, Y)$  como

$$X = \alpha^b \text{mod}(2027) = 2^b \text{mod}(2027)$$

$$Y = (\alpha^k)^b \text{mod}(2027) = (2^{1884})^b \cdot m(\text{mod}(2027)) = 13^b \cdot m(\text{mod}(2027))$$

Esto porque ya conocemos  $k$  que cumple  $\alpha^k = 13$ , que es 1884

Ahora tomamos el primer par  $(128, 793)$  y obtenemos los valores para  $b$  y  $m$  entonces

$$X = 128 = 2^b \text{mod}(2027)$$

$$\Rightarrow b = 7$$

$$Y = 793 = 13^7 \cdot m(\text{mod}(2027))$$

$$\Rightarrow m = 4$$

$$\Rightarrow (128, 793) = E$$

Obtenemos la primer letra del mensaje, E, revisando un alfabeto indexado con 26 letras (sin la Ñ). Ahora tomamos el segundo par  $(128, 528)$ , como ya conocemos que  $b = 7$  entonces basta con revisar quien es  $Y$

$$Y = 528 = 13^7 \cdot m(\text{mod}(2027))$$

$$\Rightarrow m = 18$$

$$\Rightarrow (128, 528) = S$$

Obtenemos la segunda letra del mensaje, S. Y haciendo esto para todos los demás pares obtenemos cada letra para cada par diferente:

$$(128, 793) = E$$

$$(128, 528) = S$$

$$(128, 1233) = T$$

$$(128, 264) = J$$

$$(128, 1850) = R$$

$$(128, 1410) = C$$

$$(128, 1586) = I$$

$$(128, 1762) = O$$

$$(128, 87) = A$$

$$(128, 352) = M$$

$$(128, 1938) = U$$

$$(128, 704) = Y$$

$$(128, 1498) = F$$

$$(128, 1674) = L$$

$$(128, 176) = G$$

$$(128, 1938) = U$$

$$(128, 1145) = Q$$

Con lo cual obtenemos el mensaje descifrado:

”ESTE EJERCICIO ESTA MUY FACIL AL IGUAL QUE LA TAREA”

### Ejercicio 3

Mediante el algoritmo de la criba cuadrática descomponer a  $n = 87463$

a) Encontrar B y M

Calculamos B y M de la siguiente manera:

$$B = \lfloor (e^{\sqrt{\ln(87463) \cdot \ln(\ln(87463))}})^{\frac{\sqrt{2}}{4}} \rfloor = 6$$

$$M = \lfloor (e^{\sqrt{\ln(87463) \cdot \ln(\ln(87463))}})^{\frac{3\sqrt{2}}{4}} \rfloor = 264$$

b) Dar la base, sugerencia: en la base los enteros no pasa del número 31 Escogemos la base de factorización como

$$S' = \{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$$

de donde tomamos a

$$S = \{-1, 2, 3, 13, 17, 19, 29\}$$

Esto por que cada elemento  $p \in S$  debe cumplir que  $x^2 \equiv 87463 \pmod{p}$  esto porque se debe cumplir que  $\left(\frac{n}{p}\right) = 1$ . Entonces tenemos que

$$\begin{aligned} x^2 &\equiv (87463) \pmod{3} \rightarrow 87463^1 \equiv (1) \pmod{3} \\ x^2 &\equiv (87463) \pmod{13} \rightarrow 87463^6 \equiv (1) \pmod{13} \\ x^2 &\equiv (87463) \pmod{17} \rightarrow 87463^8 \equiv (1) \pmod{17} \\ x^2 &\equiv (87463) \pmod{19} \rightarrow 87463^9 \equiv (1) \pmod{19} \\ x^2 &\equiv (87463) \pmod{29} \rightarrow 87463^{14} \equiv (1) \pmod{29} \end{aligned}$$

Y agregamos a -1 y 2 porque estos siempre son agregados a la base

c) Descomponer n

Generamos a  $m = \lfloor \sqrt{87463} \rfloor = 295$  Calculamos la tabla con  $t + 1 = 8$  relaciones de x:

i	x	q(x)	Factores de q(x)	$a_i$	$v_i$
1	1	153	$3^2 \cdot 17$	296	(0,0,1,0,1,0,0)
2	4	1938	$2 \cdot 3 \cdot 17 \cdot 19$	299	(0,1,1,0,1,1,0)
3	12	6786	$2 \cdot 3^2 \cdot 13 \cdot 29$	307	(0,1,1,1,0,0,1)
4	-17	-10179	$-3^2 \cdot 13 \cdot 29$	278	(1,0,1,1,0,0,1)
5	21	12393	$3^6 \cdot 17$	316	(0,0,1,0,1,0,0)
6	-30	-17238	$-2 \cdot 3 \cdot 13^2 \cdot 17$	265	(1,1,1,1,1,0,0)
7	52	32946	$2 \cdot 3 \cdot 17^2 \cdot 19$	347	(0,1,1,0,1,1,0)
8	-53	-28899	$-3^2 \cdot 13^2 \cdot 19$	242	(1,0,1,1,0,1,0)

Tomamos a

$$T = \{1, 5\}$$

Calculamos a  $x$  como

$$x = (a_1 \cdot a_5) \bmod(87463) = (296 * 316) \bmod(87463) = 6073$$

Calculamos todos los  $l_i$

$$l_1 = 0$$

$$l_2 = 0$$

$$l_3 = \frac{2+6}{2} = 4$$

$$l_4 = 0$$

$$l_5 = \frac{1+1}{2} = 1$$

$$l_6 = 0$$

$$l_7 = 0$$

Entonces calculamos a  $y$  como

$$y = (-1)^0 \cdot (2)^0 \cdot (3)^4 \cdot (13)^0 \cdot (17)^1 \cdot (19)^0 \cdot (29)^0 = 1377$$

Y así, vemos si se cumple que

$$x \not\equiv (y) \bmod(87463)$$

entonces proseguimos con sacar el  $MCD(x - y, n)$  debido a que se cumple que

$$6073 \not\equiv \pm(1377) \bmod(87463)$$

Entonces calculamos el

$$MCD(x - y, n) = MCD(6073 - 1377, 87463) = 587$$

$$\Rightarrow 87463 = 587 \cdot q$$

$$\Rightarrow q = 149$$

Por lo tanto:

$$n = p \cdot q$$

$$87463 = 587 \cdot 149$$

- d) Descifrar el siguiente mensaje con parámetros públicos  $(87463, 15157)$ , dar la llave privada  $d$ , recuerde el texto se tranforma módulo 26

Ya que tenemos los siguientes valores:

$$p = 857$$

$$q = 149$$

$$n = 87463$$

$$e = 15157$$

Podemos obtener los siguientes valores:

$$\begin{aligned}\phi(n) &= (p-1)(q-1) = 86728 \\ d &= 50485\end{aligned}$$

Entonces tomando el primer valor, 21347, tenemos que:

$$\begin{aligned}x_1 &= 21347^{50485} \bmod(87463) \\ x_1 &= 15 \rightarrow P\end{aligned}$$

Tomando el segundo valor, 41185, tenemos que:

$$\begin{aligned}x_2 &= 41185^{50485} \bmod(87463) \\ x_2 &= 26 \rightarrow A\end{aligned}$$

Aplicando esto para cada valor cifrado obtenemos la siguiente lista de valores:

$$\begin{aligned}
x_0 &= 21347^{50485} \bmod(87463) \\
x_0 &= 15 \rightarrow P \\
x_1 &= 41185^{50485} \bmod(87463) \\
x_1 &= 26 \rightarrow A \\
x_2 &= 31564^{50485} \bmod(87463) \\
x_2 &= 17 \rightarrow R \\
x_4 &= 76237^{50485} \bmod(87463) \\
x_4 &= 11 \rightarrow L \\
x_5 &= 73700^{50485} \bmod(87463) \\
x_5 &= 14 \rightarrow O \\
x_6 &= 53597^{50485} \bmod(87463) \\
x_6 &= 18 \rightarrow S \\
x_{13} &= 14144^{50485} \bmod(87463) \\
x_{13} &= 8 \rightarrow I \\
x_{14} &= 42561^{50485} \bmod(87463) \\
x_{14} &= 19 \rightarrow T \\
x_{17} &= 73593^{50485} \bmod(87463) \\
x_{17} &= 3 \rightarrow D \\
x_{18} &= 14420^{50485} \bmod(87463) \\
x_{18} &= 4 \rightarrow E \\
x_{22} &= 23637^{50485} \bmod(87463) \\
x_{22} &= 6 \rightarrow G \\
x_{24} &= 1^{50485} \bmod(87463) \\
x_{24} &= 1 \rightarrow B \\
x_{29} &= 2136^{50485} \bmod(87463) \\
x_{29} &= 2 \rightarrow C \\
x_{31} &= 22481^{50485} \bmod(87463) \\
x_{31} &= 12 \rightarrow M \\
x_{39} &= 82282^{50485} \bmod(87463) \\
x_{39} &= 13 \rightarrow N \\
x_{40} &= 19930^{50485} \bmod(87463) \\
x_{40} &= 20 \rightarrow U \\
x_{58} &= 67024^{50485} \bmod(87463) \\
x_{58} &= 5 \rightarrow F
\end{aligned}$$

Con lo cual podemos obtener el mensaje decifrado:

”PARA LOS PROPOSITOS DEL ALGEBRA EL CAMPO DE LOS NUMEROS REALES NO ES SUFICIENTE”

## Ejercicio 4

Demostrar con álgebra que el problema del logaritmo discreto no depende del generador

*Proof.* El problema del algoritmo discreto consiste en encontrar un  $x$  en  $\mathbb{Z}_p^*$  tal que  $\alpha^x \equiv b \pmod{p}$  con  $\alpha$  generador y  $b$  elemento de  $\mathbb{Z}_p^*$  y  $1 \leq x \leq p-1$ . Esto es igual que  $\log_\alpha b = x$ . Para demostrar que esto no depende de la base, se demostrará de acuerdo al cambio de base de las propiedades de los logaritmos.

Sean  $\alpha$  y  $\beta$  bases de  $\mathbb{Z}_p^*$ , tenemos que

$$\log_\alpha b = x \implies \alpha^x \equiv b \pmod{p}$$

$$\log_\beta b = y \implies \beta^y \equiv b \pmod{p}$$

$$\log_\alpha \beta = z \implies \alpha^z \equiv \beta \pmod{p}$$

Entonces tendríamos  $\alpha^x \equiv b \pmod{p} \equiv \beta^y \equiv (\alpha^z)^y \equiv \alpha^{zy}$  donde  $x = zy$  y por lo tanto

$$\log_\alpha b \equiv (\log_\alpha \beta) (\log_\beta b) \pmod{p}$$

Y de acuerdo a la propiedad de cambio de base, se puede calcular el mismo algoritmo con el resultado obtenido anteriormente en lugar de con la base  $\alpha$   $\square$