Sum of Two Squares

Given a prime p congruent to 1 mod 4, we will use the descent method to express p as a sum of two squares. First choose a suitable prime p:

In[11]:=
```
p=NextPrime[10000000000000000000]; While[Mod[p,4]≠1, Print[p," fails"]; p=NextPrime[p]]; Print["
```

```
10 000 000 000 000 000 051 fails
10 000 000 000 000 000 087 fails
10 000 000 000 000 000 091 fails
p = 10 000 000 000 000 000 097
```

Find a nonsquare c mod p:

In[12]:=
```
c=2; While[PowerMod[c,(p-1)/2,p]≠p-1, Print[c," fails"]; c++]; Print["c = ",c]
```

```
2 fails
c = 3
```

This allows us to write a *multiple* of p as a sum of two squares:

In[13]:=
```
a=PowerMod[c,(p-1)/4,p]; b=1; m=(a^2+b^2)/p; Print[a^HoldForm[2]," + ",b^HoldForm[2]," = ",m*p,'
```

$9\,486\,224\,609\,306\,015\,677^2 + 1 = 89\,988\,457\,338\,203\,069\,772\,888\,036\,180\,569\,768\,330 = 8\,998\,845\,733\,820\,306\,890*p$

Find smaller and smaller multiples of p expressible as a sum of two squares, until p itself is expressed as a sum of two squares:

In[14]:=
```
While[m>1, alpha=a+b*I; m=alpha*Conjugate[alpha]/p;
   a1=Mod[a,m]; If[a1>m/2, a1-=m];
   b1=Mod[b,m]; If[b1>m/2, b1-=m];
   beta=a1+b1*I; gamma=alpha*Conjugate[beta]/m;
   a=Abs[Re[gamma]]; b=Abs[Im[gamma]]; m=gamma*Conjugate[gamma]/p;
   Print[a^HoldForm[2]," + ",b^HoldForm[2]," = ",m*p," = ",m,"*p"]]
```

$513\,775\,390\,693\,984\,420^2 + 1 = 263\,965\,152\,082\,756\,332\,560\,461\,975\,202\,736\,401 = 26\,396\,515\,208\,275\,633*p$

$238\,267\,576\,814\,296\,117^2 + 19^2 = 56\,771\,438\,160\,956\,500\,550\,682\,950\,161\,278\,050 = 5\,677\,143\,816\,095\,650*p$

$7\,238\,226\,200\,436\,817^2 + 798^2 = 52\,391\,918\,528\,690\,000\,508\,201\,609\,728\,293 = 5\,239\,191\,852\,869*p$

$3\,228\,609\,003\,680\,997^2 + 1\,102\,836^2 = 10\,423\,916\,098\,650\,000\,101\,111\,986\,156\,905 = 1\,042\,391\,609\,865*p$

$997\,915\,599\,952\,388^2 + 3\,415\,483\,092^2 = 995\,835\,544\,640\,000\,009\,659\,604\,783\,008 = 99\,583\,554\,464*p$

$112\,227\,122\,880\,051^2 + 34\,226\,556\,064\,932^2 = 13\,766\,384\,250\,000\,000\,133\,533\,927\,225 = 1\,376\,638\,425*p$

$32\,375\,436\,736\,960^2 + 60\,801\,037\,623\,474^2 = 4\,744\,935\,080\,000\,000\,046\,025\,870\,276 = 474\,493\,508*p$

$24\,959\,470\,589\,509^2 + 20\,311\,087\,560\,528^2 = 1\,035\,515\,450\,000\,000\,010\,044\,499\,865 = 103\,551\,545*p$

$696\,368\,523\,231^2 + 12\,679\,714\,936\,853^2 = 161\,260\,100\,000\,000\,001\,564\,222\,970 = 16\,126\,010*p$

$4\,339\,636\,829\,546^2 + 523\,986\,820\,109^2 = 19\,107\,010\,000\,000\,000\,185\,337\,997 = 1\,910\,701*p$

$1\,774\,669\,154\,333^2 + 212\,601\,487\,904^2 = 3\,194\,650\,000\,000\,000\,030\,988\,105 = 319\,465*p$

$674\,028\,932\,628^2 + 566\,043\,282\,780^2 = 774\,720\,000\,000\,000\,007\,514\,784 = 77\,472*p$

$82\,625\,573\,371^2 + 108\,733\,686\,708^2 = 18\,650\,000\,000\,000\,000\,180\,905 = 1865*p$

$28\,594\,744\,661^2 + 63\,893\,196\,647^2 = 4\,900\,000\,000\,000\,000\,047\,530 = 490*p$

$15\,159\,277\,558^2 + 11\,840\,452\,015^2 = 370\,000\,000\,000\,000\,003\,589 = 37*p$

$383\,068\,990^2 + 8\,936\,065\,026^2 = 80\,000\,000\,000\,000\,000\,776 = 8*p$

$2\,138\,249\,009^2 + 2\,329\,783\,504^2 = 10\,000\,000\,000\,000\,000\,097 = 1*p$