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:

```
p=NextPrime[5645823652356253437584723539533265634245]; While[Mod[p,4]≠1, Print[p," fails"]; p=Nex
```

5 645 823 652 356 253 437 584 723 539 533 265 634 351 fails

p = 5 645 823 652 356 253 437 584 723 539 533 265 634 429

Find a nonsquare c mod p:

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

c = 2

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

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

$4\,280\,920\,002\,905\,268\,164\,685\,679\,799\,399\,817\,688\,716^2 + 1 =$
$18\,326\,276\,071\,274\,441\,191\,573\,023\,842\,429\,433\,360\,214\,747\,504\,166\,287\,900\,878\,717\,080\,378\,204\,273\,728\,657$
$= 3\,245\,988\,043\,502\,929\,941\,092\,002\,409\,795\,690\,682\,533 * p$

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:

```
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"]]
```

$1\,364\,903\,649\,450\,985\,272\,899\,043\,740\,133\,447\,945\,713^2 + 1 =$
$1\,862\,961\,972\,284\,618\,090\,453\,718\,935\,409\,326\,652\,286\,695\,536\,337\,575\,758\,308\,073\,327\,455\,019\,795\,078\,370$
$= 329\,971\,690\,048\,647\,049\,305\,366\,350\,529\,320\,939\,530 * p$

$186\,209\,054\,552\,312\,345\,988\,548\,578\,999\,473\,851\,577^2 + 4^2 =$
$34\,673\,811\,997\,266\,035\,223\,145\,578\,988\,446\,778\,404\,241\,762\,819\,228\,630\,578\,200\,794\,998\,163\,025\,386\,945$
$= 6\,141\,497\,526\,724\,043\,278\,235\,226\,934\,817\,101\,205 * p$

$59\,552\,015\,786\,883\,057\,928\,266\,169\,549\,050\,087\,119^2 + 120^2 =$
$3\,546\,442\,584\,281\,168\,957\,164\,898\,560\,494\,240\,318\,275\,759\,095\,895\,888\,785\,596\,752\,387\,381\,489\,734\,561$
$= 628\,153\,269\,151\,628\,683\,513\,040\,900\,225\,624\,309 * p$

$$11\,617\,847\,397\,637\,065\,600\,562\,567\,626\,492\,641\,876^2 + 11\,400^2 =$$
$$134\,974\,378\,154\,782\,337\,467\,833\,988\,649\,588\,160\,282\,820\,297\,463\,015\,695\,817\,541\,708\,770\,118\,759\,376$$
$$= 23\,906\,941\,921\,299\,919\,345\,449\,750\,008\,470\,544*p$$

$$450\,182\,895\,360\,444\,288\,684\,326\,942\,158\,317\,307^2 + 5\,540\,400^2 =$$
$$202\,664\,639\,275\,112\,731\,862\,172\,173\,139\,808\,086\,506\,974\,623\,763\,137\,793\,155\,065\,453\,727\,892\,249$$
$$= 35\,896\,381\,423\,555\,756\,959\,583\,126\,341\,581*p$$

$$79\,961\,640\,921\,613\,194\,579\,357\,925\,808\,287\,342^2 + 69\,482\,156\,400^2 =$$
$$6\,393\,864\,018\,877\,005\,817\,780\,020\,212\,027\,416\,197\,558\,824\,057\,666\,503\,953\,157\,121\,298\,384\,964$$
$$= 1\,132\,494\,461\,850\,320\,430\,925\,882\,912\,916*p$$

$$27\,928\,196\,089\,392\,080\,001\,528\,012\,478\,722\,165^2 + 4\,905\,926\,616\,934\,800^2 =$$
$$779\,984\,136\,807\,535\,070\,251\,653\,230\,991\,981\,334\,832\,943\,081\,012\,279\,986\,605\,018\,713\,327\,225$$
$$= 138\,152\,408\,724\,635\,418\,303\,159\,588\,525*p$$

$$828\,094\,802\,495\,124\,171\,823\,102\,813\,631\,146^2 + 991\,757\,595\,246\,454\,494\,000^2 =$$
$$685\,741\,001\,919\,438\,710\,307\,681\,536\,065\,694\,663\,007\,717\,121\,371\,118\,678\,221\,777\,273\,316$$
$$= 121\,459\,869\,125\,251\,277\,756\,916\,404*p$$

$$12\,550\,721\,411\,906\,902\,509\,073\,402\,228\,233^2 + 6\,761\,651\,545\,478\,254\,032\,554\,418\,000^2$$
$$= 157\,520\,653\,679\,230\,014\,866\,918\,075\,870\,810\,128\,210\,615\,096\,694\,434\,888\,146\,302\,289$$
$$= 27\,900\,385\,024\,156\,685\,578\,341*p$$

$$3\,478\,178\,048\,975\,019\,482\,528\,445\,351\,625^2 + 3\,041\,354\,323\,109\,594\,393\,378\,057\,183\,550^2$$
$$= 21\,347\,558\,659\,069\,092\,119\,122\,023\,814\,611\,367\,923\,836\,516\,110\,487\,828\,280\,743\,125$$
$$= 3\,781\,123\,884\,406\,096\,525\,625*p$$

$$1\,407\,677\,564\,174\,837\,048\,812\,944\,994\,596^2 + 604\,215\,224\,234\,058\,682\,597\,795\,474\,700^2 =$$
$$2\,346\,632\,161\,877\,416\,292\,695\,206\,253\,158\,910\,230\,817\,012\,869\,826\,488\,809\,293\,216 = 415\,640\,357\,611\,605\,929\,504*p$$

$$551\,220\,005\,262\,259\,527\,972\,720\,385\,005^2 + 433\,468\,241\,139\,047\,675\,722\,645\,095\,600^2 =$$
$$491\,738\,210\,277\,505\,005\,550\,222\,204\,022\,477\,701\,654\,404\,726\,869\,008\,568\,210\,025 = 87\,097\,692\,127\,220\,581\,725*p$$

$$82\,833\,077\,865\,552\,338\,810\,972\,167\,319^2 + 321\,810\,208\,836\,716\,335\,510\,476\,206\,460^2 =$$
$$110\,423\,129\,300\,211\,637\,441\,042\,037\,651\,894\,050\,503\,866\,145\,371\,868\,677\,379\,361 = 19\,558\,373\,782\,030\,395\,509*p$$

$$93\,947\,854\,662\,921\,109\,711\,275\,624\,167^2 + 14\,508\,492\,417\,990\,017\,205\,549\,381\,356^2 =$$
$$9\,036\,695\,748\,008\,221\,512\,939\,012\,280\,341\,926\,057\,741\,090\,219\,989\,754\,842\,625 = 1\,600\,598\,301\,407\,591\,125*p$$

$$7\,559\,371\,414\,525\,319\,603\,965\,370\,776^2 + 37\,573\,639\,172\,903\,698\,853\,717\,208\,815^2 =$$
$$1\,468\,922\,456\,878\,305\,886\,275\,392\,711\,968\,106\,328\,059\,992\,551\,465\,468\,546\,401 = 260\,178\,593\,475\,065\,269*p$$

$$11\,901\,981\,391\,676\,966\,695\,140\,813\,974^2 + 4\,224\,498\,369\,798\,285\,749\,649\,149\,010^2 =$$
$$159\,503\,547\,524\,253\,158\,753\,658\,564\,760\,670\,224\,622\,939\,331\,852\,457\,652\,776 = 28\,251\,599\,296\,355\,144*p$$

$$5\,049\,209\,756\,396\,831\,758\,338\,236\,073^2 + 2\,136\,002\,614\,668\,219\,530\,545\,766\,022^2 =$$
$$30\,057\,026\,333\,962\,423\,431\,931\,322\,779\,922\,839\,516\,769\,096\,179\,848\,165\,813 = 5\,323\,762\,870\,527\,897*p$$

$$1\,967\,358\,581\,302\,209\,123\,812\,904\,082^2 + 1\,789\,652\,999\,993\,314\,536\,026\,559\,705^2 =$$
$$7\,073\,357\,647\,808\,511\,665\,758\,072\,929\,914\,288\,641\,166\,942\,396\,461\,949\,749 = 1\,252\,847\,783\,309\,081*p$$

$$605\,937\,859\,902\,131\,301\,501\,694\,854^2 + 143\,597\,483\,259\,610\,231\,084\,697\,559^2 =$$
$$387\,780\,927\,261\,268\,941\,108\,501\,145\,218\,435\,096\,661\,173\,769\,030\,639\,797 = 68\,684\,562\,455\,193*p$$

$$217\,713\,032\,911\,859\,745\,706\,180\,535^2 + 222\,272\,511\,947\,963\,336\,910\,309\,420^2 =$$
$$96\,804\,034\,267\,338\,029\,184\,992\,687\,934\,640\,516\,616\,331\,578\,153\,622\,625 = 17\,146\,131\,411\,125*p$$

$$41\,703\,707\,289\,084\,050\,610\,112\,361^2 + 144\,157\,676\,742\,588\,494\,200\,274\,270^2 =$$
$$22\,520\,634\,965\,474\,241\,821\,543\,888\,967\,818\,272\,050\,729\,736\,269\,027\,221 = 3\,988\,901\,593\,849*p$$

$$51\,101\,666\,256\,871\,029\,869\,407\,009^2 + 975\,193\,400\,227\,878\,726\,133\,362^2 =$$
$$2\,612\,331\,296\,396\,479\,224\,567\,150\,423\,122\,021\,562\,954\,400\,707\,749\,125 = 462\,701\,539\,625*p$$

$$25\,511\,337\,122\,839\,618\,433\,796\,050^2 + 10\,763\,701\,522\,519\,057\,407\,549\,647^2 = 766\,685\,592\,261\,053\,895\,221\,102\,738\,599\,563\,960\,339\,285\,765\,427\,109 = 135\,796\,942\,921*p$$

$$16\,613\,202\,431\,120\,722\,851\,772\,856^2 + 5\,091\,672\,479\,707\,444\,465\,090\,919^2 = 301\,923\,623\,658\,005\,652\,578\,263\,796\,606\,390\,221\,472\,697\,154\,661\,297 = 53\,477\,338\,693*p$$

$$8\,153\,548\,034\,264\,550\,966\,181\,085^2 + 690\,237\,986\,468\,769\,307\,699\,197^2 = 66\,956\,774\,025\,023\,784\,138\,376\,720\,119\,216\,394\,015\,170\,846\,222\,034 = 11\,859\,522\,746*p$$

$$679\,770\,527\,226\,965\,635\,342\,708^2 + 4\,110\,199\,634\,131\,346\,808\,305\,371^2 = 17\,355\,829\,002\,099\,883\,991\,011\,978\,358\,081\,186\,979\,101\,396\,220\,905 = 3\,074\,100\,445*p$$

$$1\,505\,677\,444\,629\,822\,798\,989\,297^2 + 588\,926\,463\,041\,950\,164\,160\,644^2 = 2\,613\,898\,946\,138\,094\,593\,311\,492\,424\,477\,897\,394\,481\,759\,048\,945 = 462\,979\,205*p$$

$$102\,906\,937\,734\,359\,197\,841\,669^2 + 794\,300\,975\,991\,873\,330\,552\,009^2 = 641\,503\,878\,295\,505\,814\,006\,338\,544\,648\,250\,462\,012\,646\,641\,642 = 113\,624\,498*p$$

$$321\,269\,413\,927\,956\,447\,768\,282^2 + 98\,956\,856\,152\,816\,783\,104\,641^2 = 113\,006\,495\,705\,261\,889\,212\,756\,759\,207\,503\,170\,609\,120\,970\,405 = 20\,015\,945*p$$

$$40\,916\,465\,151\,013\,566\,258\,728^2 + 80\,425\,324\,453\,825\,637\,142\,977^2 = 8\,142\,389\,933\,957\,231\,638\,924\,375\,534\,544\,257\,098\,176\,600\,513 = 1\,442\,197*p$$

$$6\,853\,183\,293\,736\,944\,026\,618^2 + 12\,698\,720\,442\,036\,505\,994\,445^2 = 208\,223\,622\,122\,550\,983\,031\,562\,188\,861\,526\,369\,863\,375\,949 = 36\,881*p$$

$$944\,458\,303\,779\,145\,589\,052^2 + 2\,448\,653\,378\,552\,637\,927\,974^2 = 6\,887\,904\,855\,874\,629\,193\,853\,362\,718\,230\,584\,074\,003\,380 = 1220*p$$

$$615\,995\,410\,877\,078\,959\,333^2 + 1\,035\,145\,560\,988\,374\,140\,058^2 = 1\,450\,976\,678\,655\,557\,133\,459\,273\,949\,660\,049\,268\,048\,253 = 257*p$$

$$16\,633\,121\,224\,607\,672\,713^2 + 375\,325\,099\,863\,083\,819\,434^2 = 141\,145\,591\,308\,906\,335\,939\,618\,088\,488\,331\,640\,860\,725 = 25*p$$

$$127\,133\,137\,762\,898\,492\,094^2 + 186\,143\,971\,575\,138\,995\,505^2 = 50\,812\,412\,871\,206\,280\,938\,262\,511\,855\,799\,390\,709\,861 = 9*p$$

$$19\,670\,277\,937\,413\,501\,137^2 + 104\,425\,703\,112\,679\,162\,533^2 = 11\,291\,647\,304\,712\,506\,875\,169\,447\,079\,066\,531\,268\,858 = 2*p$$

$$62\,047\,990\,525\,046\,331\,835^2 + 42\,377\,712\,587\,632\,830\,698^2 = 5\,645\,823\,652\,356\,253\,437\,584\,723\,539\,533\,265\,634\,429 = 1*p$$